北京数字认证股份有限公司
全球认证体系电子认证业务规则
(CPS)

V1.0.13 版

发布日期：2025 年 11 月 26 日

生效日期：2025 年 11 月 26 日

Beijing Certificate Authority Co., Ltd.
Global Certification Practice Statement (CPS)

Version 1.0.13

Publication date: Nov 26, 2025

Effective date: Nov 26, 2025

北京数字认证股份有限公司

版本控制表

版本	状态	修订说明	审核/批准人	生效时间
1.0.1	版本发布	新版本发布	公司安全策略管理委员会	2019 年 12 月 6 日
1.0.2	版本发布	修订订户密钥对生成的规定; 增加英文译文。	公司安全策略管理委员会	2020 年 3 月 6 日
1.0.3	版本发布	更新 Mozilla 根策略、BR 及 EV 指南符合性描述; 披露 EV 证书鉴证数据源。	公司安全策略管理委员会	2021 年 1 月 20 日
1.0.4	版本发布	更新 Mozilla 根策略、BR 及 EV 指南符合性描述。	公司安全策略管理委员会	2021 年 6 月 23 日
1.0.5	版本发布	新增中级 CA 用于签发密钥长度为 RSA 3072-bit 的代码签名和时间戳证书。	公司安全策略管理委员会	2022 年 1 月 20 日
1.0.6	版本发布	更新业务符合性描述。	公司安全策略管理委员会	2022 年 7 月 25 日

1.0.7	版本发布	新增中级 CA 用于签发满足 S/MIME BR 要求的邮件证书、更新业务符合性描述。	公司安全策略管理委员会	2023 年 8 月 10 日
1.0.8	版本发布	新增中级 CA 用于签发时间戳证书、更新业务符合性描述。	公司安全策略管理委员会	2023 年 9 月 13 日
1.0.9	版本发布	新增 2 个根 CA 及其关联的下级 CA，并根据实际情况更新证书体系架构；不再签发邮件证书；更新业务符合性描述。	公司安全策略管理委员会	2024 年 3 月 1 日
1.0.10	版本发布	新增域名和 IP 验证方法；更新证书体系架构及业务符合性描述。	公司安全策略管理委员会	2024 年 8 月 27 日
1.0.11	版本发布	更新业务符合性描述。	公司安全策略管理委员会	2025 年 3 月 3 日

1.0.12	版本发布	以组合 CP/CPS 的形式，发布全球认证体系 SSL 证书 CP/CPS，更新证书体系架构及业务符合性描述。	公司安全策略管理委员会	2025 年 6 月 10 日
1.0.13	版本发布	更新业务符合性描述。	公司安全策略管理委员会	2025 年 11 月 26 日

Version Control Table

Version	Status	Revision description	Reviewed/Approved by	Effective time
Version 1.0.1	Published	New version published	Security Policy Administration Committee of Beijing Certificate Authority Co., Ltd.	December 6,2019
Version 1.0.2	Published	Revised rules for subscriber key pair generation; Add English translation.	Security Policy Administration Committee of Beijing Certificate Authority Co., Ltd.	March 6,2020
Version 1.0.3	Published	Update Mozilla root store policy, BR and EV Guidelines compliance descriptions; Disclosure of EV certificate authentication data source.	Security Policy Administration Committee of Beijing Certificate Authority Co., Ltd.	Jan 20,2021
Version 1.0.4	Published	Update Mozilla root store policy, BR and EV Guidelines compliance	Security Policy Administration Committee of Beijing Certificate Authority Co., Ltd.	Jun 23,2021

		descriptions.		
Version 1.0.5	Published	New Subordinate CAs are used to issue Code Signing Certificates and Timestamp Certificates with RSA 3072 bit key length.	Security Policy Administration Committee of Beijing Certificate Authority Co., Ltd.	Jan 20,2022
Version 1.0.6	Published	Update business compliance description.	Security Policy Administration Committee of Beijing Certificate Authority Co., Ltd.	Jul 25,2022
Version 1.0.7	Published	New Subordinate CAs are used to issue email certificates that meet S/MIME BR requirements and update business compliance description.	Security Policy Administration Committee of Beijing Certificate Authority Co., Ltd.	Aug 10,2023
Version 1.0.8	Published	New Subordinate CAs are used to issue Timestamp certificates and update business compliance description.	Security Policy Administration Committee of Beijing Certificate Authority Co., Ltd.	Sep 13,2023
Version 1.0.9	Published	New 2 Root CAs and their associated Subordinate CAs, and update the certificate	Security Policy Administration Committee of Beijing Certificate Authority Co., Ltd.	Mar 1,2024

		system architecture according to the actual situation; No longer issue email certificates; Update business compliance description.		
Version 1.0.10	Published	Add domain name and IP address validation method; Update certificate system architecture and business compliance description.	Security Policy Administration Committee of Beijing Certificate Authority Co., Ltd.	Aug 27, 2024
Version 1.0.11	Published	Update business compliance description.	Security Policy Administration Committee of Beijing Certificate Authority Co., Ltd.	Mar 3,2025
Version 1.0.12	Published	Publish global SSL CP/CPS in the form of a combined CP/CPS; Update certificate system architecture and business compliance description.	Security Policy Administration Committee of Beijing Certificate Authority Co., Ltd.	Jun 10,2025
Version 1.0.13	Published	Update business compliance description.	Security Policy Administration Committee of Beijing Certificate Authority Co., Ltd.	Nov 26,2025

声明

本 CPS 全部或者部分支持下列标准：

RFC3647：互联网 X.509 公钥基础设施-证书策略和证书业务声明框架

RFC6960：互联网 X.509 公钥基础设施-在线证书状态协议-OCSP

ITU-T X.509 V3（1997）：信息技术-开放系统互连-目录：认证框架

RFC5280：互联网 X.509 公钥基础设施证书和 CRL 结构

CA/Browser Forum BR-v2.1.9：CA/Browser 论坛 公开可信证书签发和管理的基准要求

CA/Browser Forum EV Guidelines-v2.0.1：CA/Browser 论坛 EV 证书签发管理指南

CA/Browser Forum Code Signing BR-v3.10.0：CA/Browser 论坛 公开可信代码签名证书签发和管理的基准要求

Statements

This CPS fully or partially supports the following standards:

RFC3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework

RFC6960: Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol - OCSP

ITU-T X.509 V3 (1997): Information Technology - Open System Interconnection - Catalog: Certification Framework

RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

CA/Browser Forum BR-v2.1.9: CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

CA/Browser Forum EV Guidelines-v2.0.1: CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates

CA/Browser Forum Code Signing BR-v3.10.0: CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing

Certificates

本CPS已被提交给独立的审计机构进行评估，审计评估报告将在www.bjca.cn网站及WebTrust相关网站进行公布。

This CPS has been submitted to an independent auditor for assessment. The audit report will be published on website “www.bjca.cn” and repository hosting WebTrust reports.

目录 Contents

1. 概括性描述 Introduction

1.1概述 Overview

1.1.1 公司简介 Company Profile

北京数字认证股份有限公司（Beijing Certificate Authority Co.,Ltd.，简称BJCA或“数字认证”）于2001年2月开始运营，是权威、公正的电子认证服务机构，也是首批获得中华人民共和国工业和信息化部颁发的电子认证服务许可资质的业界领先企业。数字认证公司遵照《中华人民共和国电子签名法》、《电子认证服务管理办法》的要求和相关管理规定，为用户提供数字证书申请、颁发、存档、查询、废止等服务，并通过以PKI技术、数字证书应用技术为核心的应用安全解决方案，为电子政务、电子商务、企业信息化构建安全、可靠的信任环境。2019年，数字认证公司着手实施WebTrust国际安全审计认证工作，希望以国际标准化的运营管理和服务水平，为用户提供全球化的电子认证服务。

Since February 2001, Beijing Certificate Authority Co., Ltd. (referred to as “BJCA”, or “数字认证”) has started operation as an authoritative and impartial certification authority and is one of industry leaders to be licensed as an electronic certification service provider by the Ministry of Industry and Information Technology of the People's Republic of China. Complying with the requirements and relevant regulations of *Electronic Signature Law of the People's Republic of China* and *Measures for the Administration of Electronic Certification Services*, BJCA provides users with digital certificate application, issuance, filing, inquiry, abolition and other services, and through the application security solutions with PKI technology and digital certificate application technology as the core, it builds a secure and reliable environment for e-government, e-commerce and enterprise informatization. In 2019, BJCA began to implement enhancements in the control environment for compliance with WebTrust Principles and Criteria for Certification Authorities. We aim to provide users with global electronic certification services characterized by internationally standardized operation management and service levels.

1.1.2 电子认证业务规则 Certification Practice Statement

本电子认证业务规则由数字认证公司按照中华人民共和国工业和信息化部《电子认证服务管理办法》的要求，依据《电子认证业务规则规范(试行)》制定。

This CPS is created by BJCA in accordance with the requirements of *Measures for the Administration of Electronic Certification Services* and *Standards for Electronic Certification Practice Statement (Trial)* issued by the Ministry of Industry and Information Technology of the People's Republic of China.

本电子认证业务规则适用于数字认证公司的全球认证体系 Root CA、中级 CA，以及注册机构、证书申请人、订户和依赖方等实体，涵盖了签发和管理 DV SSL 全球服务器证书、IV SSL 全球服务器证书、OV SSL 全球服务器证书、EV SSL 全球服务器证书、普通代码签名证书、EV 代码签名证书、文档签名证书、时间戳证书相关的具体操作和流程，各参与方必须完整地理解和执行本电子认证业务规则所规定的条款，并承担相应的责任和义务。

This CPS applies to BJCA's global certification system Root CA, subordinate CA, and entities including Registration Authorities (RAs), certificate applicants, subscribers and relying parties, covering specific operations and procedures related to the issuance and management of DV SSL Global Server Certificate, IV SSL Global Server Certificate, OV SSL Global Server Certificate, EV SSL Global Server Certificate, General Code Signing Certificate, EV Code Signing Certificate, Document Signing Certificate and Timestamp Certificate. Each participant shall fully understand and implement the terms and conditions set forth in this CPS and bear the corresponding responsibilities and obligations.

数字认证公司遵循国际 CA/Browser 论坛发布的《Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates》（简称“Baseline Requirements”）、《Network and Certificate System Security Requirements》（简称“NCSSR”）、《Guidelines For The Issuance And Management Of Extended Validation Certificates》（简称“EV Guidelines”）、《Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates》（简称

“Code Signing Baseline Requirements”）以及《Adobe Approved Trust List Technical Requirements》（简称“AATL Technical Requirements”）最新版本要求，定期查看其更新情况，并将持续根据其发布的版本修订本电子认证业务规则。如果本电子认证业务规则和国际 CA/Browser 论坛发布的相关规范中的条款有不一致的地方，则以国际 CA/Browser 论坛正式发布的规范为准。

BJCA follows the requirements of the latest versions of *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* ("Baseline Requirements" for short), *Network and Certificate System Security Requirements* ("NCSSR" for short), *Guidelines For The Issuance And Management Of Extended Validation Certificates* ("EV Guidelines" for short), *Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates* ("Code Signing Baseline Requirements" for short) issued by the International CA/Browser Forum and *Adobe Approved Trust List Technical Requirements* ("AATL Technical Requirements" for short), regularly review the updates and will continue to revise this CPS in accordance with the newly published versions. If there is any inconsistency between the terms of this CPS and the relevant specifications issued by the international CA/Browser forum, the specifications officially issued by the international CA/Browser forum shall prevail.

1.1.3 证书体系架构 Certificate System Architecture

本电子认证业务规则中的证书体系有 6 个根证书，分别为 BJCA Global Root CA1 证书（RSA）、BJCA Global Root CA2 证书（ECC）、BJCA Global Root CA3 证书（RSA）、BJCA Global Root CA5 G2 证书（RSA）、BJCA Global Root CA6 G2 证书（RSA）、BJCA Global Root CA7 G2 证书（RSA）。每个根 CA 下设中级 CA 签发订户证书。

The certificate system in this CPS has six Root CA Certificates, namely BJCA Global Root CA1 certificate (RSA), BJCA Global Root CA2 certificate (ECC), BJCA Global Root CA3 certificate (RSA), BJCA Global Root CA5 G2 certificate (RSA), BJCA Global Root CA6 G2 certificate (RSA) and BJCA Global Root CA7 G2 certificate

(RSA). Each Root CA Certificate has a Subordinate CA Certificate issuing subscriber certificates.

1）BJCA Global Root CA1（RSA）

根证书 Root CA	中级证书 Subordinate CA	订户证书类型 Entity Certificate Types
BJCA Global Root CA1	BJCA EV SSL CA1	EV SSL
	BJCA OV SSL CA1	OV SSL
	BJCA IV SSL CA1	IV SSL
	BJCA DV SSL CA1	DV SSL
	BJCA EV SSL CA1 G2	EV SSL
	BJCA OV SSL CA1 G2	OV SSL
	BJCA IV SSL CA1 G2	IV SSL
	BJCA DV SSL CA1 G2	DV SSL
	BJCA TimeStamp CA1	OV TimeStamp

BJCA Global Root CA1 证书的密码算法为 RSA，根密钥长度为 4096-bit，下设 9 个中级 CA 证书，其中：（1）BJCA EV SSL CA1，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 EV SSL 全球服务器证书；（2）BJCA OV SSL CA1，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 OV SSL 全球服务器证书；（3）BJCA IV SSL CA1，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 IV SSL 全球服务器证书；（4）BJCA DV SSL CA1，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 DV SSL 全球服务器证书；（5）BJCA EV SSL CA1 G2，密钥长度为 4096-bit，签发密钥长度为 RSA 2048-bit 的 EV SSL 全球服务器证书；（6）BJCA OV SSL CA1 G2，密钥长度为 4096-bit，签发密钥长度为 RSA 2048-bit 的 OV SSL 全球服务器证书；（7）BJCA IV SSL CA1 G2，密钥长度为 4096-bit，签发密钥长度为 RSA 2048-bit 的 IV SSL 全球服务器证书；（8）BJCA DV SSL CA1 G2，密钥长度为 4096-bit，签发密钥长度为 RSA 2048-bit 的 DV SSL 全球服务器证书；（9）BJCA TimeStamp CA1，密钥长度为 2048-bit，签发密钥长度为 RSA

2048-bit 的时间戳证书。

The cryptographic algorithm of the BJCA Global Root CA1 certificate is RSA with the root key size being 4096-bit, and there are 9 subordinate CA certificates, among which: (1) BJCA EV SSL CA1, the key size being 2048-bit, issuing EV SSL Global Server Certificates with the key size being RSA 2048-bit; (2) BJCA OV SSL CA1, the key size being 2048-bit, issuing OV SSL Global Server Certificates with the key size being RSA 2048-bit; (3) BJCA IV SSL CA1, the key size being 2048-bit, issuing IV SSL Global Server Certificates with the key size being RSA 2048-bit; (4) BJCA DV SSL CA1, the key size being 2048-bit, issuing DV SSL Global Server Certificates with the key size being RSA 2048-bit; (5) BJCA EV SSL CA1 G2, the key size being 4096-bit, issuing EV SSL Global Server Certificates with the key size being RSA 2048-bit; (6) BJCA OV SSL CA1 G2, the key size being 4096-bit, issuing OV SSL Global Server Certificates with the key size being RSA 2048-bit; (7) BJCA IV SSL CA1 G2, the key size being 4096-bit, issuing IV SSL Global Server Certificates with the key size being RSA 2048-bit; (8) BJCA DV SSL CA1 G2, the key size being 4096-bit, issuing DV SSL Global Server Certificates with the key size being RSA 2048-bit; (9) BJCA TimeStamp CA1, the key size being 2048-bit, issuing Timestamp Certificates with the key size being RSA 2048-bit.

BJCA Global Root CA1 根证书将于 2044 年 12 月 12 日到期。

The BJCA Global Root CA1 Root Certificate will expire on December 12, 2044.

BJCA EV SSL CA1 证书将在 2034 年 12 月 15 日到期，2025 年 6 月 15 日起，将不再使用该 CA 证书签发订户证书。

The BJCA EV SSL CA1 certificate will expire on December 15, 2034, and the CA certificate will not be used to issue subscriber certificates from June 15, 2025.

BJCA OV SSL CA1 证书将在 2034 年 12 月 15 日到期，2025 年 6 月 15 日起，将不再使用该 CA 证书签发订户证书。

The BJCA OV SSL CA1 certificate will expire on December 15, 2034, and the CA certificate will not be used to issue subscriber certificates from June 15, 2025.

BJCA IV SSL CA1 证书将在 2034 年 12 月 15 日到期，2025 年 6 月 15 日起，将不再使用该 CA 证书签发订户证书。

The BJCA IV SSL CA1 certificate will expire on December 15, 2034, and the CA certificate will not be used to issue subscriber certificates from June 15, 2025.

BJCA DV SSL CA1 证书将在 2034 年 12 月 15 日到期，2025 年 6 月 15 日起，

将不再使用该 CA 证书签发订户证书。

The BJCA DV SSL CA1 certificate will expire on December 15, 2034, and the CA certificate will not be used to issue subscriber certificates from June 15, 2025.

BJCA EV SSL CA1 G2 证书将在 2040 年 5 月 25 日到期，2037 年 5 月 25 日起，将不再使用该 CA 证书签发订户证书。

The BJCA EV SSL CA1 G2 certificate will expire on May 25, 2040, and the CA certificate will not be used to issue subscriber certificates from May 25, 2037.

BJCA OV SSL CA1 G2 证书将在 2040 年 5 月 25 日到期，2037 年 5 月 25 日起，将不再使用该 CA 证书签发订户证书。

The BJCA OV SSL CA1 G2 certificate will expire on May 25, 2040, and the CA certificate will not be used to issue subscriber certificates from May 25, 2037.

BJCA IV SSL CA1 G2 证书将在 2040 年 5 月 25 日到期, 2037 年 5 月 25 日起，将不再使用该 CA 证书签发订户证书。

The BJCA IV SSL CA1 G2 certificate will expire on May 25, 2040, and the CA certificate will not be used to issue subscriber certificates from May 25, 2037.

BJCA DV SSL CA1 G2 证书将在 2040 年 5 月 25 日到期，2037 年 5 月 25 日起，将不再使用该 CA 证书签发订户证书。

The BJCA DV SSL CA1 G2 certificate will expire on May 25, 2040, and the CA certificate will not be used to issue subscriber certificates from May 25, 2037.

BJCA TimeStamp CA1 证书将在 2034 年 12 月 15 日到期，2031 年 12 月 15 日起，将不再使用该 CA 证书签发订户证书。

The BJCA TimeStamp CA1 certificate will expire on December 15, 2034, and the CA certificate will not be used to issue subscriber certificates from December 15, 2031.

2）BJCA Global Root CA2（ECC）

根证书 Root CA	中级证书 Subordinate CA	订户证书类型 Entity Certificate Types
BJCA Global Root CA2	BJCA EV SSL CA2	EV SSL
	BJCA OV SSL CA2	OV SSL

	BJCA IV SSL CA2	IV SSL
	BJCA DV SSL CA2	DV SSL
	BJCA EV SSL CA2 G2	EV SSL
	BJCA OV SSL CA2 G2	OV SSL
	BJCA IV SSL CA2 G2	IV SSL
	BJCA DV SSL CA2 G2	DV SSL

BJCA Global Root CA2 证书的密码算法为 ECC，根密钥长度为 384-bit，下设 8 个中级 CA 证书，其中：（1）BJCA EV SSL CA2，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 EV SSL 全球服务器证书；（2）BJCA OV SSL CA2，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 OV SSL 全球服务器证书；（3）BJCA IV SSL CA2，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 IV SSL 全球服务器证书；（4）BJCA DV SSL CA2，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 DV SSL 全球服务器证书；（5）BJCA EV SSL CA2 G2，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 EV SSL 全球服务器证书；（6）BJCA OV SSL CA2 G2，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 OV SSL 全球服务器证书；（7）BJCA IV SSL CA2 G2，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 IV SSL 全球服务器证书；（8）BJCA DV SSL CA2 G2，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 DV SSL 全球服务器证书。

The cryptographic algorithm of the BJCA Global Root CA2 certificate is ECC with the root key size being 384-bit, and there are 4 subordinate CA certificates, among which: (1) BJCA EV SSL CA2, the key size being 256-bit, issuing EV SSL Global Server Certificates with the key size being ECC 256-bit; (2) BJCA OV SSL CA2, the key size being 256-bit, issuing OV SSL Global Server Certificates with the key size being ECC 256-bit; (3) BJCA IV SSL CA2, the key size being 256-bit, issuing IV SSL Global Server Certificates with the key size being ECC 256-bit; (4) BJCA DV SSL CA2, the key size being 256-bit, issuing DV SSL Global Server Certificates with the key size being ECC 256-bit; (5) BJCA EV SSL CA2 G2, the key size being 256-bit, issuing EV SSL Global Server Certificates with the key size being ECC

256-bit; (6) BJCA OV SSL CA2 G2, the key size being 256-bit, issuing OV SSL Global Server Certificates with the key size being ECC 256-bit; (7) BJCA IV SSL CA2 G2, the key size being 256-bit, issuing IV SSL Global Server Certificates with the key size being ECC 256-bit; (8) BJCA DV SSL CA2 G2, the key size being 256-bit, issuing DV SSL Global Server Certificates with the key size being ECC 256-bit.

BJCA Global Root CA2 根证书将于 2044 年 12 月 12 日到期。

The BJCA Global Root CA2 Root Certificate will expire on December 12, 2044.

BJCA EV SSL CA2 证书将在 2034 年 12 月 15 日到期，2025 年 6 月 15 日起，将不再使用该 CA 证书签发订户证书。

The BJCA EV SSL CA2 certificate will expire on December 15, 2034, and the CA certificate will not be used to issue subscriber certificates from June 15, 2025.

BJCA OV SSL CA2 证书将在 2034 年 12 月 15 日到期，2025 年 6 月 15 日起，将不再使用该 CA 证书签发订户证书。

The BJCA OV SSL CA2 certificate will expire on December 15, 2034, and the CA certificate will not be used to issue subscriber certificates from June 15, 2025.

BJCA IV SSL CA2 证书将在 2034 年 12 月 15 日到期，2025 年 6 月 15 日起，将不再使用该 CA 证书签发订户证书。

The BJCA IV SSL CA2 certificate will expire on December 15, 2034, and the CA certificate will not be used to issue subscriber certificates from June 15, 2025.

BJCA DV SSL CA2 证书将在 2034 年 12 月 15 日到期，2025 年 6 月 15 日起，将不再使用该 CA 证书签发订户证书。

The BJCA DV SSL CA2 certificate will expire on December 15, 2034, and the CA certificate will not be used to issue subscriber certificates from June 15, 2025.

BJCA EV SSL CA2 G2 证书将在 2040 年 5 月 24 日到期，2037 年 5 月 24 日起，将不再使用该 CA 证书签发订户证书。

The BJCA EV SSL CA2 G2 certificate will expire on May 24, 2040, and the CA certificate will not be used to issue subscriber certificates from May 24, 2037.

BJCA OV SSL CA2 G2 证书将在 2040 年 5 月 24 日到期，2037 年 5 月 24 日起，将不再使用该 CA 证书签发订户证书。

The BJCA OV SSL CA2 G2 certificate will expire on May 24, 2040, and the CA certificate will not be used to issue subscriber certificates from May 24, 2037.

BJCA IV SSL CA2 G2 证书将在 2040 年 5 月 24 日到期, 2037 年 5 月 24 日起，将不再使用该 CA 证书签发订户证书。

The BJCA IV SSL CA2 G2 certificate will expire on May 24, 2040, and the CA certificate will not be used to issue subscriber certificates from May 24, 2037.

BJCA DV SSL CA2 G2 证书将在 2040 年 5 月 24 日到期，2037 年 5 月 24 日起，将不再使用该 CA 证书签发订户证书。

The BJCA DV SSL CA2 G2 certificate will expire on May 24, 2040, and the CA certificate will not be used to issue subscriber certificates from May 24, 2037.

3）BJCA Global Root CA3（RSA）

根证书 Root CA	中级证书 Subordinate CA	订户证书类型 Entity Certificate Types
BJCA Global Root CA3	BJCA DocSign CA3	IV/OV DocSign
	BJCA TimeStamp CA3	OV TimeStamp

BJCA Global Root CA3 证书的密码算法为 RSA，根密钥长度为 4096-bit，下设 2 个中级 CA 证书，其中：（1）BJCA DocSign CA3，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的文档签名证书；（2）BJCA TimeStamp CA3，密钥长度为 4096-bit，签发密钥长度为 RSA 2048-bit 的时间戳证书。

The cryptographic algorithm of the BJCA Global Root CA3 certificate is RSA with the root key size being 4096-bit, and there is 2 subordinate CA certificate, among which: (1) BJCA DocSign CA3, the key size being 2048-bit, issuing Document Signing Certificates with the key size being RSA 2048-bit; (2) BJCA TimeStamp CA3, the key size being 4096-bit, issuing Timestamp Certificates with the key size being RSA 2048-bit.

BJCA Global Root CA3 根证书将于 2044 年 12 月 12 日到期。

The BJCA Global Root CA3 Root Certificate will expire on December 12, 2044.

BJCA DocSign CA3 证书将在 2034 年 12 月 15 日到期，2031 年 12 月 15 日起，将不再使用该 CA 证书签发订户证书。

The BJCA DocSign CA3 certificate will expire on December 15, 2034, and the CA certificate will not be used to issue subscriber certificates from December 15, 2031.

BJCA TimeStamp CA3 证书将在 2038 年 9 月 1 日到期, 2035 年 9 月 1 日起，将不再使用该 CA 证书签发订户证书。

The BJCA TimeStamp CA3 certificate will expire on September 1, 2038, and the CA certificate will not be used to issue subscriber certificates from September 1, 2035.

4）BJCA Global Root CA5 G2（RSA）

根证书 Root CA	中级证书 Subordinate CA	订户证书类型 Entity Certificate Types
BJCA Global Root CA5 G2	BJCA Code Signing CA5 G2	IV/OV Code Signing
	BJCA EV Code Signing CA5 G2	EV Code Signing

BJCA Global Root CA5 G2 证书的密码算法为 RSA，根密钥长度为 4096-bit，下设 2 个中级 CA 证书，其中：（1）BJCA Code Signing CA5 G2，密钥长度为 4096-bit，签发密钥长度为 RSA 3072-bit 的代码签名证书；（2）BJCA EV Code Signing CA5 G2，密钥长度为 4096-bit，签发密钥长度为 RSA 3072-bit 的 EV 代码签名证书。

The cryptographic algorithm of the BJCA Global Root CA5 G2 certificate is RSA with the root key size being 4096-bit, and there is 2 subordinate CA certificate, among which: (1) BJCA Code Signing CA5 G2, the key size being 4096-bit, issuing Code Signing Certificates with the key size being RSA 3072-bit; (2) BJCA EV Code Signing CA5 G2, the key size being 4096-bit, issuing EV Code Signing Certificates with the key size being RSA 3072-bit.

BJCA Global Root CA5 G2 根证书将于 2039 年 7 月 8 日到期。

The BJCA Global Root CA5 G2 Root Certificate will expire on July 8, 2039.

BJCA Code Signing CA5 G2 证书将在 2038 年 7 月 8 日到期，2035 年 7 月 8

日起，将不再使用该 CA 证书签发订户证书。

The BJCA Code Signing CA5 G2 certificate will expire on July 8, 2038, and the CA certificate will not be used to issue subscriber certificates from July 8, 2035.

BJCA EV Code Signing CA5 G2 证书将在 2038 年 7 月 8 日到期，2035 年 7 月 8 日起，将不再使用该 CA 证书签发订户证书。

The BJCA EV Code Signing CA5 G2 certificate will expire on July 8, 2038, and the CA certificate will not be used to issue subscriber certificates from July 8, 2035.

5）BJCA Global Root CA6 G2（RSA）

根证书 Root CA	中级证书 Subordinate CA	订户证书类型 Entity Certificate Types
BJCA Global Root CA6 G2	BJCA TimeStamp CA6 G2	OV TimeStamp

BJCA Global Root CA6 G2 证书的密码算法为 RSA，根密钥长度为 4096-bit，下设 1 个中级 CA 证书：BJCA TimeStamp CA6 G2，密钥长度为 4096-bit，签发密钥长度为 RSA 3072-bit 的时间戳证书。

The cryptographic algorithm of the BJCA Global Root CA6 G2 certificate is RSA with the root key size being 4096-bit, and there is 1 subordinate CA certificate: BJCA TimeStamp CA6 G2, the key size being 4096-bit, issuing Timestamp Certificates with the key size being RSA 3072-bit.

BJCA Global Root CA6 G2 根证书将于 2049 年 7 月 5 日到期。

The BJCA Global Root CA6 G2 Root Certificate will expire on July 5, 2049.

BJCA TimeStamp CA6 G2 证书将在 2039 年 7 月 8 日到期，2036 年 7 月 8 日起，将不再使用该 CA 证书签发订户证书。

The BJCA TimeStamp CA6 G2 certificate will expire on July 8, 2039, and the CA certificate will not be used to issue subscriber certificates from July 8, 2036.

6）BJCA Global Root CA7 G2（RSA）

根证书 Root CA	中级证书 Subordinate CA	订户证书类型 Entity Certificate Types
BJCA Global Root CA7 G2	BJCA Code Signing CA7 G2	IV/OV Code Signing

	BJCA EV Code Signing CA7 G2	EV Code Signing

BJCA Global Root CA7 G2 证书的密码算法为 RSA，根密钥长度为 4096-bit，下设 2 个中级 CA 证书，其中：（1）BJCA Code Signing CA7 G2，密钥长度为 4096-bit，签发密钥长度为 RSA 3072-bit 的代码签名证书；（2）BJCA EV Code Signing CA7 G2，密钥长度为 4096-bit，签发密钥长度为 RSA 3072-bit 的 EV 代码签名证书。

The cryptographic algorithm of the BJCA Global Root CA7 G2 certificate is RSA with the root key size being 4096-bit, and there is 2 subordinate CA certificate, among which: (1) BJCA Code Signing CA7 G2, the key size being 4096-bit, issuing Code Signing Certificates with the key size being RSA 3072-bit; (2) BJCA EV Code Signing CA7 G2, the key size being 4096-bit, issuing EV Code Signing Certificates with the key size being RSA 3072-bit.

BJCA Global Root CA7 G2 根证书将于 2039 年 7 月 8 日到期。

The BJCA Global Root CA7 G2 Root Certificate will expire on July 8, 2039.

BJCA Code Signing CA7 G2 证书将在 2038 年 7 月 8 日到期，2035 年 7 月 8 日起，将不再使用该 CA 证书签发订户证书。

The BJCA Code Signing CA7 G2 certificate will expire on July 8, 2038, and the CA certificate will not be used to issue subscriber certificates from July 8, 2035.

BJCA EV Code Signing CA7 G2 证书将在 2038 年 7 月 8 日到期，2035 年 7 月 8 日起，将不再使用该 CA 证书签发订户证书。

The BJCA EV Code Signing CA7 G2 certificate will expire on July 8, 2038, and the CA certificate will not be used to issue subscriber certificates from July 8, 2035.

1.2文档名称与标识 Document Name and Identification

本文档名称是《北京数字认证股份有限公司全球认证体系电子认证业务规则》（以下简称“本 CPS”或本《电子认证业务规则》）。

The name of this document is Certification Practice Statement of Beijing Certificate Authority Co., Ltd.'s Global Certification System (hereinafter referred to as "this CPS" or this Certification Practice Statement).

数字认证公司向国家 OID 注册管理中心注册了相应的对象标识符（OID），本文档涉及到的证书 OID 如下：

EV SSL 全球服务器证书定义的 OID 为 1.2.156.112562.2.2.11 及 2.23.140.1.1（EV Guidelines 要求）；

OV SSL 全球服务器证书的 OID 为 1.2.156.112562.2.2.12 及 2.23.140.1.2.2（Baseline Requirements 要求）；

IV SSL 全球服务器证书的 OID 为 1.2.156.112562.2.2.13 及 2.23.140.1.2.3（Baseline Requirements 要求）；

DV SSL 全球服务器证书的 OID 为 1.2.156.112562.2.2.14 及 2.23.140.1.2.1（Baseline Requirements 要求）；

EV 代码签名证书的 OID 为 1.2.156.112562.2.2.15 及 2.23.140.1.3（Code Signing Baseline Requirements 要求）；

OV 代码签名证书的 OID 为 1.2.156.112562.2.2.16 及 2.23.140.1.4.1（Code Signing Baseline Requirements 要求）；

IV 代码签名证书的 OID 为 1.2.156.112562.2.2.17 及 2.23.140.1.4.1（Code Signing Baseline Requirements 要求）；

OV 文档签名证书的 OID 为：1.2.156.112562.2.2.21;

IV 文档签名证书的 OID 为：1.2.156.112562.2.2.22;

时间戳证书用于文档签名的 OID 为：1.2.156.112562.2.2.23;

时间戳证书用于代码签名的 OID 为：1.2.156.112562.2.2.24 及 2.23.140.1.4.2（Code Signing Baseline Requirements 要求）。

BJCA has registered object identifiers (OID) with National OID Registration Management Center and the certificate OIDs involved in this document are specified

as follows:

The OID of the EV SSL Global Server Certificate is 1.2.156.112562.2.2.11 and 2.23.140.1.1 (as per EV Guidelines);

The OID of the OV SSL Global Server Certificate is 1.2.156.112562.2.2.12 and 2.23.140.1.2.2 (as per Baseline Requirements);

The OID of the IV SSL Global Server Certificate is 1.2.156.112562.2.2.13 and 2.23.140.1.2.3 (as per Baseline Requirements);

The OID of the DV SSL Global Server Certificate is 1.2.156.112562.2.2.14 and 2.23.140.1.2.1 (as per Baseline Requirements);

The OID of the EV Code Signing Certificate is 1.2.156.112562.2.2.15 and 2.23.140.1.3 (as per Code Signing Baseline Requirements);

The OID of the OV Code Signing Certificate is 1.2.156.112562.2.2.16 and 2.23.140.1.4.1 (as per Code Signing Baseline Requirements);

The OID of the IV Code Signing Certificate is 1.2.156.112562.2.2.17 and 2.23.140.1.4.1 (as per Code Signing Baseline Requirements);

The OID of the OV Document Signing Certificate is: 1.2.156.112562.2.2.21;

The OID of the IV Document Signing Certificate is: 1.2.156.112562.2.2.22;

The OID of the Timestamp Certificate for document signing is: 1.2.156.112562.2.2.23;

The OID of the Timestamp Certificate for code signing is: 1.2.156.112562.2.2.24 and 2.23.140.1.4.2 (as per Code Signing Baseline Requirements).

本 CPS 以中英文双语形式发布，若英文版本与中文版本出现任何歧义，以中文版本为准。

This document is the Chinese -English bilingual edition of BJCA CPS. In case any inconsistency or conflict between the Chinese and English versions, the Chinese version shall prevail for all purposes.

1.3PKI 参与者 PKI Participants

1.3.1 电子认证服务机构 Certification Authorities

电子认证服务机构是受用户信任，负责证书的创建、颁发、撤销和管理的权威机构，为从事电子交易活动的各方主体颁发数字证书、提供数字证书验证服务。

A certification authority is an authoritative body that is trusted by users and is responsible for the creation, issuance, revocation and management of certificates. It issues digital certificates and provides digital certificate verification services for all parties involved in electronic transaction activities.

数字认证公司是依法设立的第三方电子认证服务机构（简称“CA 机构”），符合《中华人民共和国电子签名法》、《电子认证服务管理办法》等规定。

BJCA is a third-party certification authority ("CA" for short) established in accordance with the law, and complies with *Electronic Signature Law of the People's Republic of China* and *Measures for the Administration of Electronic Certification Services*.

1.3.2 注册机构 Registration Authorities

注册机构作为电子认证服务机构授权委托的下属机构，包括注册系统（简称：RA 系统）和证书本地受理点，负责受理证书申请。

As a subordinate authority authorized by the certification authority, the RA includes the RA system ("RA system" for short) and the local certificate receiving points, responsible for receiving the certificate application.

数字认证公司除了承担 CA 机构的角色外，将自行担任 RA 注册机构，不委托第三方担任 RA 注册机构，授权的注册机构即由本 CA 机构担任。

Besides acting as a CA, BJCA will also act as a RA and no third party will be entrusted as the RA, i.e. the authorized RA shall be the CA.

1.3.3 订户 Subscribers

订户是从 CA 机构接收数字证书的实体，可以是个人、机构或设备。订户通常需要同 CA 机构签订合约以获得数字证书，并承担作为证书订户的责任。

A subscriber is an entity that receives digital certificates from a CA and can be an individual, an organization, or a device. A subscriber usually needs to contract with the CA to obtain a digital certificate and assume responsibilities as a certificate subscriber.

1.3.4 依赖方 Relying Parties

依赖方是为某一应用而使用、信任本 CA 机构签发的证书的实体。依赖方可以是、也可以不是一个订户。

A relying party is an entity that uses and trusts the certificates issued by the CA for an application. The relying party may or may not be a subscriber.

1.3.5 其他参与者 Other Participants

其他参与者指为 CA 证书服务体系提供相关服务的其他实体。

Other participants refer to other entities that provide related services for the CA certificate service system.

1.4证书应用 Certificate Usage

1.4.1 适合的证书应用 Appropriate Certificate Uses

本 CA 机构签发的数字证书适合应用在企业信息化、电子政务、电子商务及公共服务等领域，以实现身份认证、电子签名、关键数据加密等目的，同时也确保互联网信息传递双方身份的合法性和真实性、信息的完整性和保密性。

The digital certificates issued by the CA are appropriate for application in the fields of enterprise informationization, e-government, e-commerce, public services, etc., in order to achieve identity authentication, electronic signature, crucial data encryption, etc., and also to ensure the identity legality and authenticity for both parties of Internet information transmission, as well as the integrity and confidentiality of the information.

本 CA 机构的数字证书包含 SSL 全球服务器证书、代码签名证书、时间戳证书、文档签名证书，具体如下：

The digital certificates of this CA include SSL Global Server Certificates, Code Signing Certificates, Timestamp Certificates and Document Signing Certificates, specified as follows:

a. SSL 全球服务器证书

a. SSL Global Server Certificates

按照所签发证书的安全等级、鉴别方式等不同，SSL 全球服务器证书包括：DV SSL 全球服务器证书、IV SSL 全球服务器证书、OV SSL 全球服务器证书、EV SSL 全球服务器证书。DV SSL 全球服务器证书只验证网站域名所有权、控制权，不验证网站域名所有者的真实身份，可以保证网站的信息从用户浏览器到服务器之间的传输是高强度加密传输的；IV SSL 全球服务器证书专门针对个人网站经营者的网站域名所有权、控制权及个人网站经营者的真实身份进行验证；OV SSL 全球服务器证书除了验证网站域名所有权、控制权，还会对网站域名所属机构的真实身份进行验证；EV SSL 全球服务器证书则是经过更加严格的身份验证后签发的一种扩展验证型服务器证书，其验证流程符合 CA/Browser 论坛制订的增强型身份验证标准(EV Guidelines) 。

Based on different security levels and authentication methods of the issued certificates, the SSL Global Server Certificates include: DV SSL Global Server Certificates, IV SSL Global Server Certificates, OV SSL Global Server Certificates and EV SSL Global Server Certificates. The DV SSL Global Server Certificate only verifies the ownership and control of the website domain name, and does not verify the true identity of the website domain name owner, which can ensure the high-intensity encrypted transmission of the website information from the user's browser to the server; the IV SSL Global Server Certificate is specifically designed to verify the ownership and control of website domain name and the true identity of the personal website operator; in addition to verifying the ownership and control of website domain name, the OV SSL Global Server Certificate also verifies the true identity of the organization to which the website domain name belongs; the EV SSL Global Server Certificate is an extended validation server certificate issued after more strict verification, and its verification procedure conforms to the Extended Validation standard (EV Guidelines) established by the CA/Browser Forum.

SSL 全球服务器证书可用于验证证书中标识的网络主机服务器或互联网域名拥有者的身份，同时该类证书还用于订户浏览器与 WEB 服务器之间建立安全通道，实现数据信息在客户端和服务器之间的加密传输，防止数据信息的泄露。

适合应用在网上银行、电子商务、电子政务、企业信息化以及公共服务等各个领域，为建设网络可信空间提供基础性信任服务。

The SSL Global Server Certificate can be used to verify the identity of the network host server or Internet domain name owner identified in the certificate, and meanwhile, this kind of certificate can also be used to establish a secure channel between the subscriber's browser and the WEB server to realize encrypted transmission of data information between the client and the server so as to prevent disclosure of data information. It is suitable for application in various fields such as online banking, e-commerce, e-government, enterprise informationization, public services, etc., and provides basic trust services for building trusted cyberspace.

b. 代码签名证书

b. Code Signing Certificates

按照所签发证书的安全等级、鉴别方式等不同，代码签名证书包括：IV 代码签名证书、OV 代码签名证书、EV 代码签名证书。IV 代码签名证书专门针对软件开发者的个人真实身份进行验证；OV 代码签名证书专门针对开发及发布软件的机构的真实身份进行验证；EV 代码签名证书则是经过更加严格的身份验证后签发的一种扩展验证型代码签名证书，其验证流程符合 CA/Browser 论坛制订的增强型身份验证标准(Code Signing Baseline Requirements) 。

Based on different security levels and authentication methods of the issued certificates, the Code Signing Certificates include: IV Code Signing Certificates, OV Code Signing Certificates and EV Code Signing Certificates. The IV Code Signing Certificate specifically verifies the true identity of the software developer; the OV Code Signing Certificate specifically verifies the true identity of the organization that develops and publishes the software; the EV Code Signing Certificate is an extended validation Code Signing Certificate issued after more strict identity verification, and its verification procedure conforms to the Extended Validation standard (Code Signing Baseline Requirements) established by the CA/Browser Forum.

代码签名证书可用于验证证书中标识的软件代码提供方或发布方的身份，以及代码发行中的签名，以保护代码的完整性和安全性。

The Code Signing Certificates can be used to verify the identity of the software code provider or publisher identified in the certificate, as well as the signature in the code publish to protect the integrity and security of the code.

c. 时间戳证书

c. Timestamp Certificates

时间戳证书包括：OV 时间戳证书。

The Timestamp Certificates include: OV Timestamp Certificates.

OV 时间戳证书主要用于时间戳服务器，提供数字签名的功能。

The OV Timestamp Certificates are mainly used in the timestamp server and provide the function of digital signature.

d. 文档签名证书

d. Document Signing Certificates

按照所签发证书的安全等级、鉴别方式等不同，文档签名证书包括：IV 文档签名证书、OV 文档签名证书。

Based on different security levels and authentication methods of the issued certificates, the Document Signing Certificates include: IV Document Signing Certificates and OV Document Signing Certificates.

文档签名证书适用于需要确保文档的真实性、完整性和机密性的应用。PDF 文档签名证书符合 AATL Technical Requirements 相关要求，签名后的 PDF 文档使用 Adobe Reader 或 Adobe Acrobat 打开时，能自动获取可信身份并显示签名是否有效。

Document Signing Certificates are suitable for applications that need to ensure the authenticity, integrity and confidentiality of the document. The PDF Document Signing Certificate complies with the AATL Technical Requirements. When the signed PDF document is opened with Adobe Reader or Adobe Acrobat, it can automatically obtain a trusted identity and display whether the signature is valid.

1.4.2 限制的证书应用 Prohibited Certificate Uses

在本信任体系下的证书根据其类型在功能上有所限制，比如 EV SSL 服务器证书只能用于经过严格认证的 WEB 服务器。

The certificates in this trust system are functionally limited based on different types. For example, the EV SSL server certificates can only be used for strictly certified WEB servers.

各类证书的密钥用法在订户证书中的扩展项中进行了限制。然而基于证书扩展项限制的有效性取决于应用软件，如果参与方不遵守相关约定，其对证书的应用超出本 CPS 限定的应用范围，将不受 CA 机构的保护。

The key usage of various certificates is limited in the extensions of subscriber certificates. However, since the limited validity of the certificate extension depends on the application software, if the participant does not comply with the relevant agreement and its application to the certificate is beyond the scope of application defined by this CPS, it will not be protected by the CA.

本 CA 机构发放的数字证书禁止在违反国家法律、法规或破坏国家安全的情况下使用，订户不得将证书用于钓鱼式攻击、欺诈网站或其他恶意犯罪行为，不得将证书用于发布任何包含或疑似包含恶意代码的程序，由此造成的法律后果由订户负责。

Any digital certificate issued by the CA is prohibited from being used in violating national laws, regulations or damaging national security. Subscribers shall not use the certificate for phishing attacks, fraudulent websites or other malicious criminal activities, and shall not use the certificate for releasing a program that contains or is suspected to contain malware, and the resulting legal consequences shall be borne by the subscriber.

1.5策略管理 Policy Administration

1.5.1 策略文档管理机构 Organization Administering the Document

本《电子认证业务规则》的管理机构是数字认证公司安全策略管理委员会。

由数字认证公司安全策略管理委员会负责本《电子认证业务规则》的制订、发布、更新等事宜。

The administrative organization of this CPS is the Security Policy Administration Committee of BJCA. The Security Policy Administration Committee of BJCA is responsible for the creation, issuance, update and other matters of this CPS.

1.5.2 联系人 Contact Person

1.5.2.1 证书问题报告 Certificate Problem Report

证书问题报告及证书撤销请求须通过以下方式提交：

（1）发邮件至：sslservice@bjca.org.cn；或

（2）致电：+86 -4009197888。

SSL 证书订户也可通过 ACME API 提交证书撤销请求，详见本 CPS 第 4.9.3.1 节。

Certificate problem reports and certificate revocation requests shall be submitted in the following ways:

(1) Send email to: sslservice@bjca.org.cn; or

(2) Call: +86 -4009197888.

SSL certificate subscribers can also submit certificate revocation requests through ACME API, please refer to section 4.9.3.1 of this CPS.

1.5.2.2CPS 问题 CPS Problem

任何有关 CPS 的问题、建议、疑问等，都可以按以下方式进行联系。

联系部门：数字认证公司运营管理部门

联系人：李先生

网站地址：http://www.bjca.cn

电子邮箱地址：cps@bjca.org.cn

联系地址：中华人民共和国北京市海淀区北四环西路 68 号 1501 号

邮政编码：100080

电话号码：+86 10-58045600

传真号码：+86 10-58045678

For any problems, suggestions, questions, etc. about this CPS, please contact in the following ways.

Contact Department: Operation Department of BJCA

Contact person: Mr. Li

Website address: http://www.bjca.cn

Email address: cps@bjca.org.cn

Address: 1501, No. 68 North Fourth Ring Road West, Haidian District, Beijing, China

Postal code: 100080

Telephone number: +86 10-58045600

Fax number: +86 10-58045678

1.5.3 决定 CPS 符合策略的机构 Organization Determining CPS Suitability for the Policy

本《电子认证业务规则》由数字认证公司安全策略管理委员会组织制定，报数字认证公司安全策略管理委员会批准实行。

This CPS is created and approved by the Security Policy Administration Committee of BJCA.

1.5.4 CPS 批准程序 CPS Approval Procedures

本《电子认证业务规则》由数字认证公司安全策略管理委员会，组织 CPS 编写小组。编写小组完成编写 CPS 草案后，由数字认证公司安全策略管理委员会组织对 CPS 草案进行初步评审。初步评审后，将 CPS 评审稿提交数字认证公司安全策略管理委员会审批。经数字认证公司安全策略管理委员会审批通过后，

在数字认证公司的网站上对外公布，并根据《电子认证服务管理办法》的规定，从对外公布之日起的三十日之内向工业和信息化部备案。

This CPS is compiled by a team organized by the Security Policy Administration Committee of BJCA. After the CPS draft is completed by the writing team, the Security Policy Administration Committee of BJCA conducts a preliminary review of the CPS draft. After the preliminary review, the reviewed CPS draft is submitted to the Security Policy Administration Committee of BJCA for approval. Upon approval of the Security Policy Administration Committee of BJCA, it will be published on the website of BJCA, and According to Measures for the Administration of Electronic Certification Services, BJCA should put the record to the Ministry of Industry and Information Technology within 30 days after the publication.

1.5.5 CPS 修订 CPS Revision

CA 机构根据国家政策法规、技术要求、标准变化及业务发展情况等及时修订本 CPS，同时还根据 CA/Browser 论坛发布的最新版本的 Baseline Requirements、NCSSR、EV Guidelines、Code Signing Baseline Requirements 和 AATL Technical Requirements 的要求及时修订本 CPS。

The CA will revise this CPS in a timely manner in accordance with national policies and regulations, technical requirements, standard changes, business development, etc., as well as the latest version of Baseline Requirements, NCSSR, EV Guidelines, Code Signing Baseline Requirements published by the CA/Browser Forum and AATL Technical Requirements.

CA 机构将对 CPS 进行严格的版本控制，并由安全策略管理委员会负责相关事宜。本 CPS 至少每年修订一次。如果无内容改动，则递增版本号、更新发布时间、生效时间及修订记录。修订后的 CPS，从对外公布之日起的三十日之内向工业和信息化部备案。

The CA will conduct strict version control of the CPS and the Security Policy Administration Committee will be responsible for related matters. This CPS is amended at least once a year. If there is no change in content, increase the version number and update the publish time, effective time and revision history. BJCA should

submit the revised CPS to the Ministry of Industry and Information Technology for the record within 30 days after the publication.

1.6定义和缩写 Definitions and Acronyms

1.6.1 定义 Definitions

术语	定义
安全策略管理委员会	数字认证公司认证服务体系内的最高策略管理监督机构和 CPS 批准机构。
电子认证服务机构	受用户信任，负责证书的创建、颁发、撤销和管理的权威机构。
注册机构	注册机构（RA）Registration Authority 具有下列一项或多项功能的实体：识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动撤销或挂起证书，处理订户撤销或挂起其证书的请求，同意或拒绝订户更新其证书或密钥的请求。但是，RA 并不签发证书（即 RA 代表 CA 承担某些任务）。
数字证书	由电子认证服务机构签名的包含证书持有者公开身份信息和公开密钥的电子文件。
证书撤销列表	一个经电子认证服务机构数字签名的列表，它指定了一系列证书颁发者认为无效的证书，也称黑名单服务。
证书策略	关于电子认证服务机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。
电子认证业务规则	关于证书电子认证服务机构在签发、管理、撤销或更新

	证书(或更新证书中的密钥)过程中所采纳的业务实践的声明。
录入员	负责录入证书申请者提交的信息，协助用户办理数字证书申请、更新、撤销等手续。
审核员	CA 机构根据业务需要设置一级或多级审核员，负责审核证书申请信息，审核通过后，批准签发证书。
CA 注销列表	一个经电子认证服务机构数字签名的列表，标记已经被注销的 CA 的公钥证书的列表，表明该 CA 及签发的证书已经无效。
公开密钥基础设施	支持公开密钥体制的安全基础设施，提供身份鉴别、加密、完整性和不可否认性服务。
私钥	经由数字运算产生的密钥，用于制作数字签名，亦可依据其运算方式，就相对应的公开密钥加密的文件或信息予以解密。
公钥	公钥是经由数字运算产生的密钥，用于验证其对应的私钥产生的数字签名。公钥可以公开，一般标示于在线数据库、存储库或其他公共目录中，使任何希望得到公钥的人都能得到。
在线证书状态协议	在线证书检查协议，可使依赖方应用软件判断某指定证书的状态。
WebTrust	针对电子认证服务机构的现行国际审计标准。
全球服务器证书	一种可以让访问者通过浏览器来验证网站真实身份的数

	字证书，通过服务器证书可以为客户端和服务端间建立具有高安全性的 SSL 加密通道。
DV SSL 全球服务器证书	域名验证型 SSL 证书，只验证网站域名所有权的简易型 SSL 证书。
OV SSL 全球服务器证书	企业验证型 SSL 证书，既要验证网站域名所有权，也要验证网站经营者（机构）的真实身份。
IV SSL 全球服务器证书	个人验证型 SSL 证书，既要验证网站域名所有权，也要验证网站经营者（个人）的真实身份。
EV SSL 全球服务器证书	增强验证型 SSL 证书，需要对网站域名所有权、网站经营者及证书申请者的真实身份进行更加严格的增强型/扩展型验证，遵循全球统一的严格身份验证标准。
代码签名证书	用于对软件代码/程序进行数字签名的证书。
EV 代码签名证书	用于对软件代码/程序进行数字签名的证书。证书颁发前需对证书申请者进行增强型/扩展型身份验证。
文档签名证书	用于对文档进行数字签名的证书。
时间戳证书	用于时间戳服务器，提供数字签名的功能。
预证书	一种可提交到证书透明度日志的签名数据结构，如 RFC6962 所定义。

Terms	Definitions
Security Policy Administration Committee	The highest policy administration and supervision organization and CPS approval organization within the certification service system of BJCA.

Certification Authority	The authority that is trusted by users and is responsible for the creation, issuance, revocation and management of certificates.
Registration Authority	The Registration Authority (RA) has one or more of the following functions: identifying and authenticating certificate applicants, accepting or declining certificate applications, voluntarily revoking or suspending certificates in certain circumstances, handling requests of certificate revocation or suspension from subscribers, accepting or declining subscribers' requests of updating their certificate or key. However, the RA does not issue a certificate (i.e., the RA represents CA to undertake certain tasks).
Digital Certificate	An electronic document signed by a CA, which contains the public identity information and public key of the certificate holder.
Certificate Revocation List	A list digitally signed by a CA that specifies a list of certificates that the certification issuer considers to be invalid, also known as a blacklist service.
Certificate Policy (CP)	A set of rules developed by a CA that indicates the applicability of a certificate to a particular community or the rules of application for different types of security requirements.
Certification Practice Statement (CPS)	A statement of the business practice adopted by a CA in the procedure of issuing, managing, revoking or updating a certificate (or updating a key in a certificate).
Entry Clerk	Responsible for entering the information submitted by the certificate applicant and assisting the user in digital certificate application, renewal, revocation, etc.
Reviewer	According to business needs, the CA sets up one or more levels of reviewers who are responsible for reviewing the certificate application information and approving the certificate issuance after the reviews.
CA Revocation List	A list digitally signed by a certification authority that marks the list of CA's revoked public key certificates, indicating that the CA and the issued certificate have been invalidated.

Public Key Infrastructure	Secure infrastructure that supports public key systems, providing identity authentication, encryption, integrity and non-repudiation services.
Private Key	A key generated by numerical operation for making a digital signature, and can be used to decrypt a file or information encrypted by the corresponding public key according to its operation mode.
Public Key	A key generated by numerical operation to verify the digital signature generated by its corresponding private key. Public keys can be disclosed, generally identified in online databases, repository, or other public directories and available to anyone who wants to obtain the public key.
Online Certificate Status Protocol	An online certificate-checking protocol that enables relying-party application software to determine the status of a given certificate.
WebTrust	Current international auditing standard for CAs.
Global Server Certificate	A digital certificate that allows visitors to verify the true identity of a website through a browser. A server certificate can be used to establish a highly secure SSL encryption channel between the client and the server.
DV SSL Global Server Certificate	Domain validation SSL Certificate, a simple SSL certificate that only verifies the ownership of website's domain name.
OV SSL Global Server Certificate	Organization Validation SSL certificate that verifies both the ownership of website's domain name and the true identity of the website operator (organization).
IV SSL Global Server Certificate	Individual validation SSL certificate that verifies both the ownership of website's domain name and the true identity of the website operator (individual).
EV SSL Global Server Certificate	Extended validation SSL certificate requires more strict extended validation of the ownership of website's domain name, the authenticity of the website operator and the certificate applicant, conforming to the rigorous validation standards which are globally unified.
Code Signing Certificate	A certificate used to digitally sign software code/programs.
EV Code Signing	A certificate used to digitally sign software code/programs.

Certificate	Extended identity verification of the certificate applicant is required before issuing the certificate.
Document Signing Certificate	A certificate used to digitally sign a document.
Timestamp Certificate	Used for timestamp servers to provide digital signatures.
Precertificate	A signed data structure that can be submitted to a Certificate Transparency log, as defined by RFC6962.

1.6.2 缩写 Acronyms

缩写 Acronyms	英文全称 English Full Name	中文全称 Chinese Full Name
CA	Certificate Authority	电子认证服务机构，证书颁发机构
RA	Registration Authority	注册审核服务机构
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则
SSL	Secure Sockets Layer	加密套接层协议
TLS	Transport Layer Security	传输层安全
CRL	Certificate Revocation List	证书撤消列表
ARL	Certificate Authority Revocation List	CA 注销列表
LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
OCSP	Online Certificate Status Protocol	在线证书状态协议
PIN	Personal Identification Number	个人身份识别码
PKCS	Public KEY Cryptography Standards	公共密钥密码标准
PKI	Public Key Infrastructure	公共密钥基础设施

RFC	Request For Comments	互联网建议标准
CAA	Certification Authority Authorization	认证机构授权
CSR	Certificate Signing Request	证书请求文件
DBA	Doing Business As	商业名称
DNS	Domain Name System	域名系统
ICANN	Internet Corporation for Assigned Names and Numbers	互联网名字与编号分配机构
EV	Extended Validation	扩展验证/增强验证
FIPS	Federal Information Processing Standards	联邦信息处理标准
FQDN	Fully Qualified Domain Name	完全限定域名
gTLD	Generic top-level domain	通用顶级域名
SCT	Signed Certificate Timestamp	已签证书时间戳
ACME	Automated Certificate Management Environment	自动化证书管理环境
API	Application Programming Interface	应用程序编程接口

2. 信息发布与信息管理 Information Publication and Administration

2.1信息库 Repositories

本 CA 机构的信息库面向订户及依赖方提供信息服务，提供信息服务包括但不限于以下内容：根证书和中级 CA 证书、CP 和 CPS 现行和历史版本、CRL、EV 证书鉴证数据源以及数字认证公司不定期发布的信息。

The CA's repository provides information services to subscribers and relying parties, and the information services include, but are not limited to, the following content: Root CA Certificates and Subordinate CA Certificates, current and historical versions

of CP and CPS, CRLs, Authentication Data Source for EV Certificates, and information irregularly issued by BJCA.

2.2认证信息的发布 Publication of Information

本 CA 机构通过官网公布以下信息：根证书和中级 CA 证书、CP 和 CPS 现行和历史版本以及其他由数字认证公司不定时发出的信息。数字认证公司官网网址：http://www.bjca.cn，是数字认证公司发布所有信息最权威的渠道，供相关方下载、查阅。

The CA publishes the following information through the official website: root certificates and subordinate CA certificates, current and historical versions of the CP and CPS, and other information irregularly published by the BJCA. The official website of BJCA, http://www.bjca.cn, is the most authoritative channel for information publication, available for the related parties to download and view.

本 CA 机构通过在线服务发布 CRL 和 OCSP 信息，订户及依赖方可以通过在线服务获取证书状态查询、证书撤销查询服务等。

The CA publishes CRL and OCSP information through the online service, so that subscribers and the relying parties can obtain the certificate status inquiry and the certificate revocation inquiry service through the online service.

本 CA 机构将“bjca.cn”作为 CAA 查询标签。

The CA uses "bjca.cn" as the CAA query label.

2.3发布的时间或频率 Time or Frequency of Publication

本 CA 机构的 CPS 按照本 CPS 第 1.5.4 节所述的批准流程，经数字认证公司安全策略管理委员会审批通过后，在数字认证公司的网站上对外公布。本 CA 机构至少每年发布一次 CP 和 CPS，CP 和 CPS 可通过信息库 7X24 小时获得。

The CPS of this CA is published on the website of BJCA after approval by the Security Policy Administration Committee in accordance with the approval procedure described in Section 1.5.4 of this CPS. The CA publishes CP and CPS at least once a year. CP and CPS are available through the repository as 7X24 service.

CA 机构发布 CRL 的频率根据证书策略确定，订户证书的 CRL 为 24 小时定期发布，订户证书 CRL 的有效期 3 天。中级 CA 的 ARL 为每 12 个月定期发布，

中级证书 ARL 的有效期 12 个月。如果根证书被撤销，应及时在网站公布撤销信息。

The frequency at which the CA publishes CRL is determined according to the Certificate Policy. The CRL of the subscriber certificate is published periodically every 24 hours and is valid for 3 days. The subordinate CA's ARL is published periodically every 12 months and is valid for 12 months. Information should be published on website timely if a Root CA Certificate is revoked.

在特殊情况下，CA 机构可以提前进行证书和 CRL 的发布。

In special conditions, CA can issue certificates and publish CRLs in advance.

2.4信息库访问控制 Access Controls on Repositories

对于公开发布的 CP、CPS 和 CA 证书等公开信息，本 CA 机构允许公众自行通过网站以只读方式进行查询和访问。

For public information such as published CP, CPS and CA certificates, the CA allows the public to make inquiries and accesses through the website in a read-only manner.

CA 机构通过网络安全防护、系统安全设计、安全管理制度确保只有经过授权的人员才能对信息库中的信息进行增加、删除、修改和发布。

Through network security protection, system security design and security management system, CA ensures that only authorized personnel can add, delete, modify, and publish information in its repository.

3. 身份标识与鉴别 Identification and Authentication

3.1命名 Naming

3.1.1 名称类型 Types of Names

CA 机构颁发的数字证书符合 X.509 标准、RFC5280 标准、CA/Browser 论坛 Baseline Requirements 及 EV Guidelines 的要求，含有颁发机构和证书订户主体甄别名，每个订户对应一个甄别名（Distinguished Name，简称 DN），甄别名采用 X.500 标准命名方式，是证书持有者的唯一识别名。

The digital certificate issued by the CA complies with X.509 standard, RFC5280 standard, CA/Browser Forum Baseline Requirements and EV Guidelines, and contains the issuing authority and the distinguished name of the certificate subscriber. Each subscriber corresponds to a Distinguished Name (DN). The DN is the unique identifier of the certificate holder adopt the X.500 standard naming method.

对于 SSL/TLS 服务器证书，所有的域名或 IP 地址都添加到主题别名中，而通用名必须是一个出现在主题别名中的域名或 IP 地址。对于 EV SSL 服务器证书，所有的域名都添加到主题别名中，且添加到主题别名中的域名不能包含通配符，而通用名必须是一个出现在主题别名中的域名。

For SSL/TLS server certificates, all domain names or IP addresses are added to Subject Alternative Name, whereas the Common Name must be a domain name or IP address that exists in Subject Alternative Name. For EV SSL server certificates, all domain names are added to Subject Alternative Name, and the Common Name must be a domain name that exists in Subject Alternative Name, and the Common Name and Subject Alternative Name cannot contain wildcards.

EV SSL 证书和 EV 代码签名证书命名规则和要求必须被记录在按照 CP 制定的本 CPS 中，并符合 CA/Browser 论坛 EV Guidelines 和 Code Signing Baseline Requirements 的要求。

The naming rules and requirements of EV SSL certificates and EV Code Signing Certificates must be recorded in this CPS created in accordance with the CP and in accordance with the requirements of the EV Guidelines and Code Signing Baseline Requirements issued by the CA/Browser Forum.

本 CA 机构的 Root CA 主题甄别名命名规则：

属性	值
通用名（CN）	Root CA 名称
机构（O）	BEIJING CERTIFICATE AUTHORITY
国家（C）	CN

The naming rules of ROOT CA's DN are as follows:

Attributes	Values
commonName (CN)	Name of Root CA
organizationName (O)	BEIJING CERTIFICATE AUTHORITY
countryName (C)	CN

本 CA 机构的中级 CA 主题甄别名命名规则:

属性	值
通用名（CN）	中级 CA 名称
机构（O）	BEIJING CERTIFICATE AUTHORITY
地区（L）	颁发者所在城市（可选）
省（S）	颁发者所在省份（可选）
国家（C）	CN

The naming rules of the subordinate CA's DN are as follows:

Attributes	Values
commonName (CN)	Name of subordinate CA
organizationName (O)	BEIJING CERTIFICATE AUTHORITY
localityName（L）	The city where the issuer is located (optional)
stateOrProvinceName（S）	The state where the issuer is located (optional)
countryName (C)	CN

证书订户的主题甄别名命名规则:

属性	值
通用名（CN）	域名/IP，或订户名称，或其他可识别的名称
电子邮件（E）	订户的电子邮件地址（可选）
机构部门（OU）	可以包含以下一个或多个内容:

	订户所在机构的具体部门； 其他描述身份或证书类型的文字
机构（O）	对于有确定机构的订户，是订户所在机构名称
地区（L）	订户所在城市（可选）
省（S）	订户所在省份（可选）
国家（C）	订户所在国家，如 CN

The naming rules of certificate subscriber's DN are as follows:

Attributes	Values
commonName (CN)	Domain name/IP， or name of subscriber， or other identifiable names
emailAddress (E)	Email address of the subscriber (optional)
organizationalUnitName (OU)	May contain one or more of the following: The specific department of the organization where the subscriber is located; Other text describing the identity or certificate type
organizationName (O)	The name of the organization where the subscriber is located for those subscribers with a defined organization
localityName（L）	The city where the issuer is located (optional)
stateOrProvinceName（S）	The state where the issuer is located (optional)
countryName (C)	The country where the subscriber is located, such as CN

3.1.2 对名称意义化的要求 Need for Names to be Meaningful

订户的甄别名(DN)是标识证书主题唯一性的元素，必须具有一定的代表意义，可与证书持有者的特有属性相关联。

The subscriber's distinguished name (DN) is an element that identifies the uniqueness of the certificate's subject. It must be representative and can be associated with unique attributes of the certificate holder.

EV SSL 证书的甄别名通常包含订户所属机构拥有的域名、订户机构的企业身份信息，作为标识订户的关键信息被鉴别和认证，订户机构的企业身份信息需经过第三方严格的身份审核。

The EV SSL certificate's DN usually includes the domain name owned by the organization to which the subscriber belongs and the organization identity information of the subscriber organization, which is identified and authenticated as the key information of subscriber identity. The organization identity information of the subscriber organization is subject to strict third-party identity verification.

OV SSL 证书的甄别名通常包含订户所属机构拥有的域名或公网 IP，以及订户机构的企业身份信息，作为标识订户的关键信息被鉴别和认证，订户机构的企业身份信息需经过第三方严格的身份审核。

The OV SSL certificate's DN usually includes the domain name owned by the organization to which the subscriber belongs or public IP address, and the organization identity information of the subscriber organization, which is identified and authenticated as the key information of subscriber identity. The organization identity information of the subscriber organization is subject to strict third-party identity verification.

IV SSL 证书的甄别名通常包含订户拥有的域名或公网 IP，以及订户的个人身份信息，作为标识订户的关键信息被鉴别和认证，订户的个人身份信息需经过第三方严格的身份审核。

The IV SSL certificate's DN usually includes the domain name owned by the subscriber or public IP address, and the individual identity information of the subscriber, being identified and authenticated as the key information of subscriber identity. The individual identity information of the subscriber is subject to strict third-party identity verification.

DV SSL 证书的甄别名通常仅包含订户所属机构拥有的域名或公网 IP，作为标识订户的关键信息被认证。

The DV SSL certificate's DN usually only contains the domain name owned by the organization to which the subscriber belongs or public IP address, being authenticated as the key information of subscriber identity.

EV 代码签名证书的甄别名通常包含订户机构的企业身份信息，作为标识订户的关键信息被鉴别和认证，订户机构的企业身份信息需经过第三方严格的身份审核。

The EV Code Signing Certificate's DN usually includes the organization identity information of the subscriber organization, being identified and authenticated as the key information of subscriber identity. The organization identity information of the subscriber organization is subject to strict third-party identity verification.

普通代码签名证书甄别名中的通用名通常可包含个人的真实名称或组织机构名称，作为标识订户的关键信息被认证。

The Common Name in the DN of the General Code Signing Certificate usually contains personal real name or organization name, which is authenticated as the key information of subscriber identity.

文档签名证书甄别名中的通用名通常可包含个人的真实名称或组织机构名称，作为标识订户的关键信息被认证。

The Common Name in the DN of the Document Signing Certificate usually contains personal real name or organization name, which is authenticated as the key information of subscriber identity.

OV 时间戳证书甄别名中的通用名通常可包含组织机构名称，作为标识订户的关键信息被认证。

The Common Name in the DN of the OV Timestamp Certificate usually contains organization name, which is authenticated as the key information of subscriber identity.

3.1.3 订户的匿名或伪名 Anonymity or Pseudonymity of Subscribers

在本 CA 机构的全球认证体系中，订户(证书申请人)不能使用匿名或伪名。

In the global certification system of this CA, subscribers (certificate applicants) shall not be anonymous or pseudo.

3.1.4 理解不同名称形式的规则 Rules for Interpreting Various Name Forms

CA 机构签发的数字证书符合 X.509 V3 标准，甄别名格式遵守 X.500 标准。甄别名的命名规则由数字认证公司定义。甄别名（DN）的具体内容依次由 CN、OU、O、C 四部分组成。其中 CN 用来表示用户名，OU、O 用来表示组织单位名称、C 用来表示国家。

The digital certificate issued by the CA complies with X.509 V3 standard, and the DN's format complies with X.500 standard. The naming rules for DN are defined by BJCA. The specific content of the DN consists of four parts: CN, OU, O and C, wherein CN is used to indicate the user name, OU and O are used to indicate the organization unit name, and C is used to represent the country.

3.1.5 名称的唯一性 Uniqueness of Names

在本 CA 机构的全球认证体系中，证书主题名称必须是唯一的。但对于同一订户，可以用其主题名为其签发多张证书，但证书的扩展项不同。当证书申请中出现不同订户存在相同名称时，遵循先申请者优先使用，后申请者增加附加识别信息予以区别的原则。

In the global certification system of this CA, the certificate's subject name must be unique. However, for the same subscriber, its subject name can be used to issue multiple certificates with different extensions. When different subscribers have the same name during certificate application, the principle is that the first applicant has the priority to use the name, and the latter applicants add additional identification information for differentiation.

3.1.6 商标的识别、鉴别和角色 Recognition, Authentication, and Role of Trademarks

数字认证公司尊重任何订户名称中的注册商标权，任何证书申请者不应使用任何可能侵犯知识产权的名称。证书信息中包含商标时，订户应向数字认证公司提供商标注册方所有权的文件证明，这种要求不是也不应该被认为是数字认证公司将对商标的归属进行判断和决定。

BJCA respects the registered trademark rights in any subscriber name, and any certificate applicant shall not use any name that may infringe intellectual property rights. When the certificate information contains a trademark, the subscriber shall provide BJCA with a documentary proof of the ownership of the trademark registrant. This requirement is not and shall not be considered as a judgment or decision by BJCA on the attribution of the trademark.

数字认证公司不负责解决证书中任何关于域名、商标等知识产权的纠纷，并且不保证这种权利的唯一性。对于因商标、服务标志等的归属问题造成的纠纷，数字认证公司没有权力，也没有义务去拒绝或者质疑任何可能导致产生知识产权纠纷的证书申请，不负有仲裁或调停等责任，但保留撤销任何涉及知识产权争议的证书的权利。

BJCA is not responsible for resolving any disputes concerning intellectual property rights such as domain names and trademarks in the certificate, and does not warrant the uniqueness of such rights. For disputes arising from the attribution of trademarks, service marks, etc., BJCA has no power and no obligation to refuse or query any certificate application that may lead to intellectual property disputes, and does not bear the responsibility of arbitration or mediation, but retains the right of revoking any certificate involving intellectual property disputes.

3.2初始身份确认 Initial Identity Validation

3.2.1 证明拥有私钥的方法 Method to Prove Possession of Private Key

证书申请者必须证明持有与所注册公钥相对应的私钥，证明方法包括：PKCS#10、其它与此相当的密钥标识方法，或者 CA 机构接受的其它证明方式。

The certificate applicant shall prove the possession of the 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 CA.

3.2.2 机构身份和域名的鉴别 Authentication of Organization and Domain Identity

订户申请数字认证公司在该信任体系下签发的证书前应由证书申请人，提供有效身份证明文件、证书申请文件，并接受证书申请的有关条款，同意承担相应的责任。

Before the subscriber applies for the certificate issued by BJCA under this trust system, the certificate applicant shall provide valid identity documents and certificate application documents, accept the relevant provisions of certificate application, and agree to bear corresponding responsibilities.

CA 机构或注册机构接受订户的证书申请后，应对订户的身份真实性进行审核，并按照双方的约定妥善保存订户申请材料。

After accepting the certificate application of the subscriber, the CA or RA shall authenticated the subscriber's identity and properly keep the subscriber's application materials in accordance with the agreement of both parties.

3.2.2.1 机构身份的鉴别 Authentication of Organization Identity

机构订户在申领证书前应持机构有效身份证件，包括但不限于：营业执照、法人代码证、事业单位法人证书、社会团体登记证书、民办非企业登记证书、外

国（地区）企业常驻代表机构登记证和政府批文，提出证书申请。

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

CA 机构或授权的注册机构将确认机构订户是确实存在的、合法的实体及确认申请人的意愿。其鉴别流程方法如下。

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

（1）通过权威第三方数据库对有效机构身份证明文件进行核查确认，确保所提供的信息与核查结果一致。

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

（2）检查组织机构授权给授权代表办理证书事宜的授权文件及授权代表有效身份证件，确保授权代表得到申请机构的授权。CA 机构可通过鉴证数据源得到的电话号码等方式与申请机构进行联络，以确认申请者某个信息的真实性，如验证申请表中的某个人是否是授权代表。

(2) Check the authorization documents authorized by the organization to the authorized representative to handle the certificate and the valid government-issued photo ID of the authorized representative to ensure that the authorized representative is authorized by the organization. The CA can contact the applicant through a telephone number obtained by Authentication Data Source to confirm the authenticity of some information of the applicant, such as verifying whether a person in the application form is an authorized representative.

（3）通过手机短信、银行打款附言等方式，与证书申请人核实证书请求，确认申请人的真实意愿。

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

（4）如果 CA 机构无法从第三方得到所有所需的信息，可委托第三方进行调查或要求申请者提供额外的信息和证明材料。

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

CA机构建立和维护证书高风险申请人列表，在接受证书申请时会查询该列表，对于列表中出现的申请人，CA机构将拒绝其申请。

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

3.2.2.2DBA/商业名称的鉴别 Authentication of DBA/Tradename

若证书主题中包含DBA或商业名称，CA机构或授权的注册机构将通过以下方式中的至少一种确认申请者有权使用该DBA或商业名称。

If the certificate subject contains a DBA or tradename, the CA or the authorized RA shall verify the applicant’s right to use the DBA or tradename using at least one of the following ways.

（1）政府机构提供的可证明申请者合法成立、存在或认可的有效文档。

（2）可靠的数据来源。（如：邓白氏编码、商务部对外贸易经营者备案）

（3）其他本 CA 机构认为可靠的验证方式。

(1) Valid documents provided by a government agency in the jurisdiction of the applicant’s legal creation, existence, or recognition.

(2) A reliable data source. (eg: Dun & Bradstreet, Ministry of Commerce Foreign trade operator registration)

(3) Other DBA/Tradename's authentication methods that the CA determines to be reliable.

3.2.2.3 国家的鉴别 Verification of Country

若证书主题中包含国家选项，CA机构或授权的注册机构将通过以下方式中

的至少一种进行国家的鉴别。

If the certificate subject contains an option of country, the CA or the authorized RA shall verify the country using one of the following ways.

（1）通过权威第三方数据库查询网站DNS记录显示的IP地址或申请者的IP地址来确认所在国，确保申请人的IP地址所在国与申请人实际所在国一致。

（2）请求域名的ccTLD。

（3）域名注册机构提供的信息。

（4）通过本CPS第3.2.2.1节中申请者提供的机构证明信息进行所在国家的确认。

(1) Confirm the host country by checking the IP address displayed by the DNS record of the website or the IP address of the applicant through an authoritative third-party database, and ensure that the country where the applicant's IP address is located is consistent with the actual country where the applicant is located.

(2) The ccTLD of the requested domain name.

(3) Information provided by the domain name registrar.

(4) Confirm the country through the information provided by the applicant in Section 3.2.2.1 of this CPS.

3.2.2.4 域名的确认和鉴别 Verification and Authentication of Domain Name

参见全球认证体系SSL证书策略和电子认证业务规则。

See Global SSL Certificate Policy and Certification Practice Statement.

3.2.2.5IP 地址的确认和鉴别 Verification and Authentication of an IP Address

参见全球认证体系SSL证书策略和电子认证业务规则。

See Global SSL Certificate Policy and Certification Practice Statement.

3.2.2.6 通配符域名的确认和鉴别 Verification and Authentication of

Wildcard Domain Names

参见全球认证体系SSL证书策略和电子认证业务规则。

See Global SSL Certificate Policy and Certification Practice Statement.

3.2.2.7 数据源的准确性 Data Source Accuracy

CA机构将EV证书鉴证数据源在官方网站上公布，如有需要，请访问https://www.bjca.cn。

The CA publicly discloses Authentication Data Source for EV Certificates on the official website. If necessary, please visit https://www.bjca.cn.

CA机构在变更证书鉴证数据源之后，应及时披露EV证书鉴证数据源的最新版本。

The CA shall disclose the latest version of Authentication Data Source for EV Certificates in a timely manner after changing the certificate authentication data source.

在将任何数据源作为可靠的数据源之前，CA机构对该来源的可靠性、准确性及更改或伪造可抗性进行评估，遵守CA/Browser论坛Baseline Requirements第3.2.2.7 节对数据源的要求，并考虑以下因素：

Prior to use any data source as a reliable data source, the CA shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification, comply with CA/Browser Forum Baseline Requirements section 3.2.2.7 for data source requirements, taking into account the following factors:

（1）所提供信息的年限。

（2）信息来源的更新频率。

（3）数据供应商和数据收集的目的。

（4）数据对公众的可用性及可访问性。

（5）伪造或改变数据的相对难度。

(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.

对于所签发的订户证书，若从评估为可依赖数据来源中获得的数据或文件的时间不超过本 CPS 第 6.3.2 节中约定的证书最大有效期，则本 CA 机构可使用该数据及文件。对于根据本 CPS 第 3.2.2.9 节获得的邮箱控制权验证数据，重用验证数据或文件的时间不超过证书签发前 30 天。

For the issued subscriber certificate, the data and documents may be used by the CA if the time of obtaining data or documents from data source evaluated as reliable does not exceed the maximum validity period of the certificate as specified in Section 6.3.2 of this CPS. For mailbox control validation data obtained in accordance with Section 3.2.2.9 of this CPS, the reuse of verification data or files shall not exceed 30 days before the certificate is issued.

3.2.2.8 认证机构授权（CAA）Certification Authority Authorization (CAA)

参见全球认证体系SSL证书策略和电子认证业务规则。

See Global SSL Certificate Policy and Certification Practice Statement.

3.2.2.9 邮件地址的确认和鉴别 Verification and Authentication of Email Address

CA机构或授权的注册机构将对申请者邮件地址的有效性和控制权进行鉴别。其鉴别流程方法如下。

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

（1）通过邮件方式发送随机值，然后接收一个使用该随机值的确认响应，确认申请人对邮箱的控制权。对每个邮箱的控制权应使用一个唯一的随机值进行确认。随机值应仅发送到正在验证的电子邮件地址，不得以任何其他方式共享。

（2）申请者收到邮件并回复该随机值进行确认。

（3）CA 机构收到回复，并将回复中的随机值与发送的随机值进行比对，若结果一致，则邮件地址鉴别通过。

(1) Send a random value by email, and receive a confirming response using the random value to confirm the applicant's control over the mailbox. Control over each Mailbox Address SHALL be confirmed using a unique Random Value. The Random Value SHALL be sent only to the email address being validated and SHALL not be shared in any other way.

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

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

上述鉴别方法中用到的随机值的有效期为从产生该随机值开始的 24 小时内。

The random value used in the above validation method is valid for no more than 24 hours from the time of its creation.

3.2.2.10 DV SSL 全球服务器证书订户身份鉴别 Authentication of DV SSL Global Server Certificate Subscriber Identity

参见全球认证体系SSL证书策略和电子认证业务规则。

See Global SSL Certificate Policy and Certification Practice Statement.

3.2.2.11 IV SSL 全球服务器证书订户身份鉴别 Authentication of IV SSL Global Server Certificate Subscriber Identity

参见全球认证体系SSL证书策略和电子认证业务规则。

See Global SSL Certificate Policy and Certification Practice Statement.

3.2.2.12 OV SSL 全球服务器证书订户身份鉴别 Authentication of OV SSL Global Server Certificate Subscriber Identity

参见全球认证体系SSL证书策略和电子认证业务规则。

See Global SSL Certificate Policy and Certification Practice Statement.

3.2.2.13 EV SSL 全球服务器证书订户身份鉴别 Authentication of EV SSL Global Server Certificate Subscriber Identity

参见全球认证体系SSL证书策略和电子认证业务规则。

See Global SSL Certificate Policy and Certification Practice Statement.

3.2.2.14 普通代码签名证书订户身份鉴别 Authentication of General Code Signing Certificate Subscriber Identity

个人订户、机构订户如需要申请普通代码签名证书，可以向CA机构或授权的注册机构提交申请。订户申请普通代码签名证书时，应提交如下纸质或电子数据形式申请材料:

If the subscribers of organizations and individuals apply for a General Code Signing Certificate, they may apply to the CA or an authorized RA. When a subscriber applies for a General Code Signing Certificate, the following paper or electronic data materials shall be submitted:

1、证书申请表

2、至少一种机构信息证明材料（个人订户不适用）

3、申请人的个人身份证明材料

4、机构授予申请人的授权证明（个人订户不适用）

1. Certificate application form

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

3. Applicant's personal identification proof

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

CA 机构除对订户身份进行鉴别外，还要对 CSR 合规性进行鉴别。其鉴别流程方法如下。

（1）若证书的甄别名中包含个人真实名称/组织机构名称，按照本 CPS 第

3.2.3 节/第 3.2.2.1 节进行身份鉴别。

（2）对于 CSR 文件的鉴别主要包含：CSR 中的信息是否与申请表中的申请信息一致，如 CSR 申请信息与申请表中的不一致，则以申请表为准；是否符合相关规范，比如 DN 的顺序等；验证其是否拥有私钥。

In addition to the identification of the subscriber, the CA also needs to authenticate the CSR compliance. The authentication procedure is specified as follows.

(1) If the certificate's distinguished name contains the personal name/organization name, the identity is authenticated in accordance with Section 3.2.3/3.2.2.1 of this CPS.
(2) The authentication of the CSR file mainly includes whether the information in the CSR is consistent with the application information in the application form. If the CSR application information is inconsistent with the application form, the application form shall prevail; whether the relevant specifications, such as the order of the DN, are met; verify that it has a private key.

CA 机构不对申请订户的代码进行鉴别。

The CA does not identify the code of the applicant subscriber.

代码签名证书必须被保存在满足 FIPS 140-2 安全规格或相应级别的安全介质中，介质包括但不限于智能密码钥匙 USBKey、加密机等，可采取的分发方式包括:

1、 CA 机构为订户生成代码签名证书并保存在满足 FIPS 140-2 Level 2 安全规格的智能密码钥匙 USBKey 中，由 CA 机构邮寄给订户。

2、 订户自己在安全介质中生成密钥对，将生成密钥对的相关 log、生成密钥对的设备具体型号、CSR 文件提供给本 CA 机构以供审核。

The Code Signing Certificate must be kept in a secure medium that meets FIPS 140-2 security specifications or a corresponding level. Media includes, but is not limited to, a smart key USB key, an encryptor, etc., and the available distribution methods include:

1. The CA generates a Code Signing Certificate for the subscriber and keeps it in the smart key USBKey that meets the FIPS 140-2 Level 2 security specifications, which

is mailed to the subscriber by the CA.

2. The subscriber generates a key pair on the security medium, and provides the relevant log of the key pair, the specific model of the device that generated the key pair, and the CSR file to the CA for audit.

3.2.2.15 EV 代码签名证书订户身份鉴别 Authentication of EV Code Signing Certificate Subscriber Identity

机构订户如需要申请EV 代码签名证书，可以向CA机构或授权的注册机构提交申请。EV代码签名证书申请，不能包括域名或IP地址。申请者只能是国家机关、企事业单位、社会团体等机构订户。且申请机构需要满足如下条件：

If the subscriber applying for an EV Code Signing Certificate is an organization, it may apply to the CA or an authorized RA. EV Code Signing Certificate application cannot include domain names or IP addresses. Applicant subscribers can only be organizations such as Government Entity, Business Entity, and Private Organization. And the applicant organizations need to meet the following conditions:

1、国家机关应满足如下条件：

（1）经由上级按照其职能批准建立；

（2）在订户申请材料中必须明确单位的授权代表；

（3）所在国家允许 CA 签发证书；

（4）不在任何政府拒绝名单或禁止名单（如贸易禁运）中。

1. Government Entity shall meet the following conditions:

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

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

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

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

2、企事业单位应满足如下条件：

（1）获得当地监管机构承认的合法组织；

（2）不在监管机构的“停业”、“无效”、“过期”名单之列；

（3）在订户申请材料中必须明确单位的授权代表；

（4）拥有固定的营业场所；

（5）机构和授权代表所在国家允许 CA 签发证书；

（6）机构和授权代表不在任何政府拒绝名单或禁止名单（如贸易禁运）中。

2. Business Entity shall meet the following conditions:

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

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

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

(4) Have a fixed place of business;

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

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

3、社会团体应满足如下条件：

（1）获得当地监管机构承认的合法组织；

（2）不在监管机构的“停业”、“无效”、“过期”名单之列；

（3）在订户申请材料中必须明确单位的授权代表；

（4）拥有固定的营业场所；

（5）所在国家允许 CA 签发证书；

（6）不在任何政府拒绝名单或禁止名单（如贸易禁运）中。

3. Private Organization shall meet the following conditions:

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

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

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

(4) Have a fixed place of business;

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

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

4、申请机构应拥有的角色：

申请人：申请单位经办人员

审批人：申请单位主管人员

签署人：申请协议的签署人

申请代理人：在 CA 与申请者是关联方，且双方有适用于 EV 证书使用准则的情况下，申请者需设定申请代理人，代表申请者认可证书的使用准则。

证书申请机构可授权一个人来完成所有的角色，也可分别多人来完成。以上角色必须是申请单位的职员或被授权的代理人，申请单位需确认申请角色的信息真实准确并以 CA 机构认可的方式（包括但不限于注册公章、注册法人人名章、角色签名等方式）对证书申请及订户协议进行签名，对于不实的申请角色信息，CA 机构有权拒绝申请，并对已发放的证书进行撤销。

CA 机构通过电话、手机短信、有回执的邮政信函或其它同等方式与申请角色进行核实确认，以验证其对证书申请及订户协议签名的真实性。

4. The role that the applicant organization shall have:

Certificate Requestor: handling personnel of the application unit

Certificate Approver: the person in charge of the application unit

Contract Signer: Signatory of the application agreement

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

The certificate applicant organization can authorize one person or multiple people to fulfil all the roles. Above roles must be employees or authorized agents of the

applicant. The applicant shall confirm that the information of the application role is true and accurate, and sign the certificate request and subscriber agreement in the way approved by CA (including but not limited to the registered official seal, registered legal person's name seal, role signature, etc.). For the false information of the application role, the CA has the right to refuse the application and withdraw the issued certificate.

The CA shall verify and confirm with the application role by phone, SMS, postal letter with receipt or other equivalent methods to verify the authenticity of its certificate request and subscriber agreement signature.

5、订户申请 EV 代码签名证书时，应提交如下纸质或电子数据形式申请资料：

（1）EV 证书申请表

（2）至少一种机构信息证明材料

（3）至少两种申请人的身份证明材料

（4）机构授予申请人的授权证明

（5）企业存在证明文件

5. When a subscriber applies for an EV Code Signing Certificate, the following paper or electronic data materials shall be submitted:

(1) EV Certificate application form

(2) At Least One Organization Information Proof

(3) At least two types of Certificate Requestor's identification proof

(4) Proof of authorization granted by the organization to the applicant

(5) Proof of company’s existence

EV 代码签名证书申请的鉴别方法：

Identification methods for EV Code Signing Certificate Application are as followed:

（1）订户身份鉴别

a. 验证申请机构的身份合法性

通过 EV 证书鉴证数据源查询申请机构注册编码（如统一社会信用代码）真伪；验证申请机构身份信息及注册地址；

必须直接通过合格的独立信息来源进行验证。

b. 对机构验证的内容

申请机构身份信息是否存在;

申请机构身份信息是否准确;

申请机构提供的经营地址是否与注册文件（如营业执照）中登记的注册地址一致;

通过物业账单、银行对账单、政府出具的税务文件或其他 CA 机构认为可靠的验证方式验证申请机构的经营地址及注册地址信息。

c. 验证申请机构的存续状态

通过 EV 证书鉴证数据源查询申请机构注册编码（如统一社会信用代码），验证其是否正常存续或查询申请机构提供的银行验资报告验证机构存续状态。

d. 对 EV 证书申请相关人员的身份验证

EV 证书申请人（个体工商户申请 EV 证书时，证书申请人需是经营者本人）必须经过面对面（视频）的方法进行验证;

通过公安部身份核验平台验证身份信息;

通过拨打固定电话（必须是通过鉴证数据源得到的公司电话）与申请机构人事部门联系，确认申请人、审批人、签署人的人员身份及授权。

(1) Subscriber identity authentication

a. Verify the legality of the applicant organization

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

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

b. Content of organization verification

Whether the identity information of the applicant organization exists;

Whether the identity information of the applicant organization is accurate;

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

Verify the business address and registered address information of the applicant organization through property bills, bank statements, government-issued tax bills, or other verification methods deemed reliable by the CA.

c. Verify operational existence of the applicant organization

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

d. Authentication of EV certificate applicant's principal individua

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

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

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

（2）CSR 文件鉴别

对订户提交的 CSR 文件内容进行验证，检查 CSR 中的信息是否与申请表中的信息一致，是否符合相关规范，并验证其是否拥有私钥。

(2) CSR file authentication

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

（3）EV 代码签名证书分发控制

EV 代码签名证书必须被保存在满足 FIPS 140-2 安全规格或相应级别的安全介质中，介质包括但不限于智能密码钥匙 USBKey、加密机等，可采取的分发方

式包括:

1、 CA 机构为订户生成代码签名证书并保存在满足 FIPS 140-2 Level 2 安全规格的智能密码钥匙 USBKey 中，由 CA 机构邮寄给订户。

2、 订户自己在安全介质中生成密钥对，将生成密钥对的相关 log、生成密钥对的设备具体型号、CSR 文件提供给本 CA 机构以供审核。

(3) EV Code Signing Certificate distribution control

The EV Code Signing Certificate must be kept in a secure medium that meets FIPS 140-2 security specifications or a corresponding level. The media include, but are not limited to, a smart key USBkey, an encryptor, etc., and the available distribution methods include:

1. The CA generates a Code Signing Certificate for the subscriber and keeps it in the smart key USBKey that meets the FIPS 140-2 Level 2 security specifications, which is mailed to the subscriber by the CA.

2. The subscriber generates a key pair on the security medium, and provides the relevant log of the key pair, the specific model of the device that generated the key pair, and the CSR file to the CA for audit.

3.2.2.16 时间戳证书订户身份鉴别 Authentication of Timestamp Certificate Subscriber Identity

机构订户如需要申请时间戳证书，可以向CA机构或授权的注册机构提交申请。订户申请时间戳证书时，应提交如下纸质或电子数据形式申请材料:

If the subscriber applying for a Timestamp Certificate is an organization, it may apply to the CA or an authorized RA. When a subscriber applies for a Timestamp Certificate, the following paper or electronic data materials shall be submitted:

1、证书申请表

2、至少一种机构信息证明材料

3、申请人的个人身份证明材料

4、机构授予申请人的授权证明

1. Certificate application form

2. At Least One Organization Information Proof

3. Applicant's personal identification proof

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

CA 机构除对订户身份进行鉴别外，还要对 CSR 合规性进行鉴别。其鉴别流程方法如下。

（1）按照本 CPS 第 3.2.2.1 节的要求鉴别订户机构身份。

（2）对于 CSR 文件的鉴别主要包含：CSR 中的信息是否与申请表中的申请信息一致，如 CSR 申请信息与申请表中的不一致，则以申请表为准；是否符合相关规范，比如 DN 的顺序等；验证其是否拥有私钥。

In addition to the identification of the subscriber, the CA also needs to authenticate the CSR compliance. The authentication procedure is specified as follows.

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

(2) The authentication of the CSR file mainly includes whether the information in the CSR is consistent with the application information in the application form. If the CSR application information is inconsistent with the application form, the application form shall prevail; whether the relevant specifications, such as the order of the DN, are met; verify that it has a private key.

3.2.2.17 文档签名证书订户身份鉴别 Authentication of Document Signing Certificate Subscriber Identity

个人订户、机构订户如需要申请文档签名证书，可以向 CA 机构或授权的注册机构提交申请。订户申请文档签名证书时，应提交如下纸质或电子数据形式申请材料：

If the individuals and organizations apply for Document Signing Certificates, they may apply to the CA or an authorized RA. When a subscriber applies for a Document Signing Certificate, the following paper or electronic data materials shall be submitted:

1、证书申请表

2、至少一种机构信息证明材料（个人订户不适用）

3、申请人的个人身份证明材料

4、机构授予申请人的授权证明（个人订户不适用）

1. Certificate application form

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

3. Applicant's personal identification proof

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

CA 机构除对订户身份进行鉴别外，还要对 CSR 合规性进行鉴别。其鉴别流程方法如下。

（1）若证书的甄别名中包含个人真实名称/组织机构名称，按照本 CPS 第 3.2.3 节/第 3.2.2.1 节进行身份鉴别。

（2）对于 CSR 文件的鉴别主要包含，CSR 中的信息是否与申请表中的申请信息一致，是否符合相关规范，比如 DN 的顺序等，并验证其是否拥有私钥。

In addition to the identification of the subscribe, CA also needs to authenticate the CSR compliance. The authentication procedure is specified as follows.

(1) If the certificate's distinguished name contains the personal name/organization name, the identity is authenticated in accordance with Section 3.2.3/3.2.2.1 of this CPS.

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

文档签名证书必须被保存在满足 FIPS 140-2 安全规格或相应级别的安全介质中，介质包括但不限于智能密码钥匙 USBKey、加密机等，可采取的分发方式包括:

1、 CA 机构为订户生成文档签名证书并保存在满足 FIPS 140-2 Level 2 安全规格

的智能密码钥匙 USBKey 中，由 CA 机构邮寄给订户。

2、 订户自己在安全介质中生成密钥对，将生成密钥对的相关 log、生成密钥对的设备具体型号、CSR 文件提供给本 CA 机构以供审核。

The Document Signing Certificate must be kept in a secure medium that meets FIPS 140-2 security specifications or a corresponding level. The media include, but are not limited to, a smart key USBkey, an encryptor, etc., and the available distribution methods include:

1. The CA generates a Document Signing Certificate for the subscriber and keeps it in the smart key USBKey that meets the FIPS 140-2 Level 2 security specifications, which is mailed to the subscriber by the CA.
2. The subscriber generates a key pair on the security medium, and provides the relevant log of the key pair, the specific model of the device that generated the key pair, and the CSR file to the CA for audit.

3.2.3 个人身份的鉴别 Authentication of Individual Identity

个人订户或机构订户申请人在申领证书前应持个人有效身份证件，包括但不限于：身份证、户口簿、军官证、港澳居民来往内地通行证、台胞证、护照和外国人永久居留证等，提出证书申请。

To submit a certificate application, individuals or organizations authorized representative shall hold valid government-issued photo ID before applying for a certificate, including but not limited to: ID card, residence booklet, military ID, Mainland Travel Permit for Hong Kong and Macau Residents, Taiwan Compatriot Travel Certificate, passport and permanent resident permit for foreigners.

CA 机构或授权的注册机构将确认个人身份的真实性和有效性。其鉴别流程方法如下。

（1）通过权威第三方数据库对有效身份证明文件进行核查确认，确保所提供的信息与核查结果一致。

（2）通过手机短信、银行打款附言等方式，与个人订户核实证书请求。必要时可通过语音、视频、拍照、面对面等方式对个人订户的身份进行确认。

（3）当申请信息包含机构信息时，需要确认该机构是否存在，以及申请人是否属于该机构的成员。

（4）在域名、设备名称或者邮件地址被作为证书主题内容申请证书时，还需要验证该个人申请者是否拥有该权利，例如要求提交域名所有权文件、归属权证明文件或者申请者对所有权的书面承诺等。

The CA or authorized RA shall confirm the authenticity and validity of the individual's identity. The authentication procedure is specified as follows.

(1) Check and confirm the valid government-issued photo IDs through an authoritative third-party database to ensure that the provided information is consistent with the verification results.

(2) Verify the certificate request with an individual subscriber by SMS, postscript of bank payment, etc. If necessary, the identity of the individual subscriber can be confirmed by voice call, video call, photo taking, face to face meeting, etc.

(3) When the application information contains organizational information, it is necessary to confirm whether the organization exists and whether the applicant is a member of the organization.

(4) When the domain name, device name or email address is used as the certificate subject content to apply for a certificate, it is also necessary to verify whether the individual applicant has the right, for example, requesting the domain name ownership document, the ownership certificate or the applicant's written commitment to ownership, etc.

CA机构建立和维护证书高风险申请人列表，在接受证书申请时会查询该列表，对于列表中出现的申请人，CA机构将拒绝其申请。

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

3.2.4 没有验证的订户信息 Non-verified Subscriber Information

若订户提交鉴证文件不属于鉴别范围内的信息，为没有验证的订户信息。证书中的信息必须经过验证，未经验证的信息不得写入证书。

Non-verified subscriber information refers to the information submitted by the subscriber beyond the scope of authentication. The information in the certificate must be verified and non-verified information shall not be included into the certificate.

3.2.5 授权确认 Validation of Authority

为确保办理人具有特定的许可，代表组织获取数字证书，需要提供组织授权其代表该组织为办理 CA 数字证书事宜的授权文件。组织在 CA 机构的数字证书申请表上加盖单位公章后，则证明本组织对办理人的授权确认。

In order to ensure that the agent has a specific license to represent the organization to obtain a digital certificate, an authorization document that the organization authorizes the agent to represent the organization for the CA digital certificate needs to be provided. After the organization affixes the official seal of the unit on the digital certificate application form of the CA, it proves that the organization has confirmed the authorization of the person in charge.

本 CA 机构允许申请者指定独立个人来申请证书。若申请者以书面形式指定了可以进行证书申请的独立个人，则不接受在该指定人员以外的任何证书申请请求。在收到申请者已核实的书面请求时，应向申请者提供其已授权人员的清单。

The CA allows an applicant to specify the independent individuals who may request certificates. If an applicant specifies, in writing, the independent individuals who may request a certificate, then the CA shall not accept any certificate requests that are outside this specification. The CA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6 互操作准则 Criteria for Interoperation or Certification

本 CA 机构可以与其他电子认证服务机构进行互操作，要求该电子认证服务机构的 CP 及 CPS 必须符合北京数字认证股份有限公司全球认证体系证书策略的要求，并与数字认证公司签署相关协议。

The CA can interoperate with other certification authorities, and require that their CP and CPS shall confirm to the requirements of the CP of global certification system of

Beijing Certificate Authority Co.,Ltd., and the relevant agreement shall be signed with BJCA.

如果国家法律法规对其有要求，数字认证公司将严格遵守。

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

截至目前，本 CA 机构未签发任何交叉认证的证书。

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

3.3密钥更新请求的标识与鉴别 Identification and Authentication for Re-key Requests

3.3.1 常规密钥更新的标识与鉴别 Identification and Authentication for Routine Re-key

在订户证书到期前，订户需获得新证书以保持证书使用的连续性。本 CA 机构一般要求订户产生一个新密钥对代替过期的密钥对，即视为常规密钥更新。

Prior to the expiration of the subscriber certificate, the subscriber needs to obtain a new certificate to maintain the continuity of the use of the certificate. The CA generally requires the subscriber to generate a new key pair to replace the expired key pair, which is considered as a routine re-key.

对于一般情况下的密钥更新申请，订户须提交能够识别原证书的足够信息，如订户甄别名、证书序列号等，对申请的鉴别基于：

（1）原证书存在并由 CA 机构签发；

（2）用原证书上的订户公钥对申请的签名进行验证；

（3）基于原注册信息进行身份鉴别。

For a general re-key request, the subscriber must submit sufficient information to identify the original certificate, such as the subscriber's DN, certificate serial number, etc. The identification of the application is based on :

(1) The original certificate exists, and it was issued by the CA;

(2) verifying the signature of the application with the subscriber's public key on the

original certificate;
(3) Identity authentication based on the original registration information.

密钥更新会造成使用原密钥对加密的文件或数据无法解密，订户在申请密钥更新前，须确认使用原密钥对加密的文件或数据已解密，由此造成的损失，CA 机构将不承担责任。

Re-key can cause files or data encrypted using the original key to be unable to be decrypted. The subscriber must confirm that the encrypted file or data using the original key has been decrypted before applying for the re-key, and the CA will not be liable for the losses caused thereby.

3.3.2 撤销后密钥更新的标识与鉴别 Identification and Authentication for Re-key After Revocation

证书撤销后的密钥更新等同于订户重新申请证书，则撤销后密钥更新的标识与鉴别使用初始身份确认相同的流程，其要求与本 CPS 第 3.2 节相同。

The re-key after the certificate is revoked is equivalent to the subscriber reapplying the certificate. The identification and authentication of the re-key after revocation is the same as the procedure of authenticating the initial identity. The requirements are the same as in Section 3.2 of this CPS.

3.4撤销请求的标识与鉴别 Identification and Authentication for Revocation Requests

若订户主动申请撤销证书，CA 机构将通过权威第三方数据库、手机短信、域名控制权验证等方式对订户身份进行鉴别。

If the subscriber actively applies for revocation of the certificate, the CA will verify the identity of subscribers through authoritative third-party database, SMS, domain name control verification, and other methods.

若因订户未履行本 CPS 所规定的义务或由于本 CPS 第 4.9.1.1 节所述理由，由本 CA 机构或授权的注册机构申请撤销订户的证书时，无需对订户身份进行鉴别。

If the subscriber fails to perform the obligations specified in this CPS or because of reasons stated in Section 4.9.1.1 of this CPS, the identity of the subscriber is not required to be authenticated when the CA or the authorized RA applies to revoke the subscriber's certificate.

4. 证书生命周期操作要求 Certificate Life-cycle Operational Requirements

4.1证书申请 Certificate Application

4.1.1 证书申请实体 Who Can Submit a Certificate Application

证书申请实体包括个人和具有独立法人资格的组织机构(包括国家机关、企事业单位、社会团体等)。

The certificate application entities include individuals and organizations with independent legal personality (including Government Entity, Business Entity, Private Organization, etc.).

4.1.2 注册过程与责任 Enrollment Process and Responsibilities

证书申请人按照本 CPS 所规定的要求，通过现场面对面或在线方式提交证书申请，包括相关的身份证明材料。CA 机构或注册机构受理证书申请，依据身份鉴别规范对证书申请人的身份进行鉴别，并决定是否签发证书。

The applicant shall submit the certificate application through face-to-face or online way, including relevant identification materials, in accordance with the requirements stipulated in this CPS. The CA or the RA accepts the certificate application, identifies the identity of the certificate applicant according to the identity authentication specification, and decides whether to issue the certificate.

订户：订户应事先对订户协议、本 CPS 及相关 CP 所规定的责任和义务进行了解，并确认接受。正式发起注册请求，则订户需要参照本 CPS 第 3.2 节的要求进行证书申请操作，应配合 CA 机构或授权的注册机构完成对身份信息的采集、记录和审核。注册成功后，订户有责任保护其所获得的证书私钥的安全。

Subscriber: The subscriber shall know in advance the responsibilities and obligations stipulated in the subscriber agreement, this CPS and the relevant CP, and confirm acceptance. To formally request for registration, the subscriber needs to refer to the requirements of Section 3.2 of this CPS for certificate application operations, and should cooperate with CA or an authorized RA to complete the collection, recording, and review of identity information. After successful registration, the subscriber is responsible for protecting the security of the obtained certificate private key.

根据《中华人民共和国电子签名法》的规定，证书申请人未向 CA 机构提供真实、完整和准确的信息，或者有其他过错，给 CA 机构或电子签名依赖方造成损失的，应承担相应的法律责任和经济赔偿。

According to *Electronic Signature Law of the People's Republic of China*, if the certificate applicant fails to provide true, complete and accurate information to CA, or has other faults, and causes losses to CA or relying party of the electronic signature, the certificate applicant shall bear the corresponding legal responsibility and indemnification obligations.

CA 机构：CA 机构录入员、审核员参照本 CPS 第 3.2 节及第 5.2.4 节的要求对订户的身份信息进行采集、记录，审核。通过录入员、审核员两个可信人员的鉴证审批后，CA 机构向订户签发证书。

CA: CA entry clerks and reviewer collect, record, and review the identity information of subscribers in accordance with the requirements of Sections 3.2 and 5.2.4 of this CPS. After verification and approval by two trusted persons (entry clerk and reviewer), the CA issues a certificate to the subscriber.

4.2证书申请处理 Certificate Application Processing

4.2.1 执行识别与鉴别功能 Performing Identification and Authentication Functions

CA 机构或授权的注册机构接收到订户的证书申请后，按照本 CPS 所规定的身份鉴别流程对申请人的身份进行识别与鉴别。具体的鉴别流程详见本 CPS 第 3.2 节。

After receiving the certificate application of the subscriber, the CA or the authorized

RA identifies and authenticates the identity of the applicant according to the identity authentication procedure stipulated in this CPS. The specific identification procedure is detailed in Section 3.2 of this CPS.

CA 机构会对待签发的全球服务器证书主题别名扩展项中的每一个 dNSName 做 CAA 记录检查，并按照本 CPS 第 3.2.2.8 中的检查方法和结果判定是否批准该证书申请。在全球服务器证书签发前，若 CA 机构根据本 CPS 第 3.2 节获得的数据或证明文件的时间不超过本 CPS 第 6.3.2 节中约定的服务器证书最大有效期，且该信息未发生变化，则 CA 机构可重用该数据或证明文件，对订户身份进行识别与鉴别。

The CA will perform a CAA record check for each dNSName in the certificate Subject Alternative Name extension of a Global Server Certificate to be issued, and determine whether to approve the certificate application according to the inspection method and result in Section 3.2.2.8 of this CPS. Prior to the issuance of a Global Server Certificate, if the time of obtaining data or certification by the CA under Section 3.2 of this CPS does not exceed the maximum validity period of the server certificate as specified in Section 6.3.2 of this CPS, and the information has not changed, the CA can reuse the data or supporting documents to identify and authenticate the subscriber identity.

在代码签名证书、文档签名证书签发前，若 CA 机构根据本 CPS 第 3.2 节获得的数据或证明文件的时间不超过本 CPS 第 6.3.2 节中约定的代码签名证书、文档签名证书最大有效期，且该信息未发生变化，则 CA 机构可重用该数据或证明文件，对订户身份进行识别与鉴别。

Before the Code Signing Certificate and Document Signing Certificate are issued, if the time of obtaining data or certificate by the CA according to Section 3.2 of this CPS does not exceed the maximum validity period of Code Signing Certificate and Document Signing Certificate as stipulated in Section 6.3.2 of this CPS, and the information has not changed, the CA can reuse the data or the certification file to identify and authenticate the subscriber identity.

4.2.2 证书申请批准和拒绝 Approval and Rejection of Certificate Applications

CA 机构或授权的注册机构根据本 CPS 所规定的身份鉴别流程对证书申请人身份进行识别与鉴别后，根据鉴别结果决定批准或拒绝证书申请。

After the CA or the authorized RA identifies and authenticates the identity of the certificate applicant according to the identity authentication procedure stipulated in this CPS, it decides to approve or reject the certificate application according to the identification result.

如果证书申请人通过本 CPS 所规定的身份鉴别流程且鉴证结果为合格，CA 机构或授权的注册机构将批准证书申请，为证书申请人制作并颁发数字证书。

If the certificate applicant passes the identity authentication procedure specified in this CPS and the verification result is qualified, the CA or the authorized RA will approve the certificate application and create and issue a digital certificate for the certificate applicant.

如果发生下列情形，CA 机构有权拒绝证书申请:

1) 根据本 CPS 第 3.2 节的规定，不能完成识别和认证所有必需的订户信息；

2) 订户不能根据要求提供所需要的身份证明材料；

3) 订户反对或者不能接受订户协议的有关内容和要求；

4) 订户没有或者不能够按照规定支付相应的费用；

5) 申请的证书含有 ICANN 考虑中的新顶级域名；

6) CA 机构认为批准该申请将会对数字认证公司带来争议、法律纠纷或者损失。

The CA rejects the certificate application if:

1) According to the provisions of Section 3.2 of this CPS, not all necessary subscriber information can be identified and authenticated;

2) The subscriber cannot provide the required identity documents;

3) The subscriber objected or could not accept the relevant content and requirements of the subscriber agreement;

4) The subscriber fails to or cannot pay corresponding fees as required;

5) The certificate applied for contains a new top-level domain name under consideration by ICANN;

6) The CA believes that the approval of the application will bring disputes, legal disputes or losses to BJCA.

对于拒绝的证书申请，CA 机构通知申请人证书申请失败，同时告知申请人失败的原因(法律禁止的除外)。

For the rejected certificate applications, the CA will inform the applicant of the failure of the certificate application and reasons (except where prohibited by law).

CA 机构根据反钓鱼联盟、防病毒厂商或相关联盟、负责网络安全事务的政府机构等第三方发布的名单，或公共媒体公开报道中披露的信息，建立和维护证书高风险申请人列表，在接受证书申请时会查询该列表，对于列表中出现的申请人，CA 机构将拒绝其申请。对于已签发的证书，会定期根据列表予以复核，一旦发现证书持有人出现在列表中，CA 机构有权撤销该证书或采取适当机制进行处理。

The CA establishes and maintains certificates high risk applicants list according to the list published by the anti-phishing Alliance, antivirus vendors or related Union, government agencies responsible for network security services, or information disclosed in public reports by media, and will check the list when accepting certificate applications. For applicants in the list, the CA will reject the application. For issued certificates, they will be reviewed periodically according to the list. Once the certificate holder is found in the list, the CA has the right to revoke the certificate or take appropriate mechanism to deal with it.

对于法律法规、国家政府部门、行业监管部门或当地政府明确禁止从事商业活动或其它公开活动的机构，CA 机构有权拒绝为其签发证书。此外，如果证书申请相关人员（包括申请人、审批人、签署人、申请代理人等）受到法律法规、国家或地方政府的相关限制，CA 机构拒绝受理由其参与的证书申请事宜。

For those organizations is prohibited engaging in commercial activities or public activities by laws and regulations, national government departments, industry regulators, the CA has the right to refuse issuing an certificate. In addition, if the person (including Certificate Requestor, Certificate Approver, Contract Signer, Applicant Representative, etc.) applying for the certificate is subject to relevant laws and regulations, national or local government restrictions, the CA may refuse to accept the certificate application in which the person is involved.

4.2.3 处理证书申请的时间 Time To Process Certificate Applications

CA 机构或授权的注册机构将做出合理努力来尽快确认证书申请信息，一旦注册机构收到了所有必须的相关信息，将在下一个工作日内受理，并在 3-5 个工作日完成审核与证书签发。

The CA or the authorized RA will make reasonable efforts to confirm the certificate application information as soon as possible. Once the RA has received all necessary relevant information, it will start processing in the next working day, and complete the audit and certificate issuance in 3-5 working days.

CA 机构或授权的注册机构能否在上述时间期限内处理证书申请取决于证书申请人是否真实、完整、准确地提交了相关信息和是否及时地响应了 CA 的管理要求。

Whether the CA or the authorized RA can process the certificate application within the above time limit depends on whether the applicant has submitted the relevant information in a true, complete and accurate manner and whether it has responded to the management requirements of the CA in a timely manner.

4.3证书签发 Certificate Issuance

4.3.1 证书签发中注册机构和电子认证服务机构的行为 RA and CA Actions During Certificate Issuance

根 CA 的证书签发由本 CA 机构授权的可信人员谨慎地发布直接指令，使根

CA 执行证书签名操作。

Certificate issuance by the Root CA Certificate shall require a trusted person authorized by the CA to deliberately issue a direct command in order for the Root CA Certificate to perform a certificate signing operation.

在订户证书的签发过程中，CA 机构的录入员负责录入证书申请者提交的信息，审核员负责证书申请的审批，并通过操作 RA 系统将签发证书的请求发往 CA 的证书签发系统。RA 发出的证书签发请求信息需有注册机构的身份鉴别与信息保密措施，并确保请求发到正确的 CA 机构。

During the issuance process of the subscriber certificate, the entry clerk of the CA is responsible for entering the information submitted by the applicant, and the reviewer is responsible for the approval of the application, and the request for certificate is sent to the CA certificate issuance system by operating the RA system. The certificate issuance request information issued by the RA requires the identity authentication and information security measures of the RA, and ensures that the request is sent to the right CA.

CA 机构在获得证书签发请求后，判断证书签发请求的有效性，在批准证书申请之后，将签发证书。对于 SSL 全球服务器证书的签发，在申请 SCT 数据之前，将对预证书进行 linting 工具检测并结合错误信息的人工复核，以防止签发违反 Baseline Requirements 要求的证书。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

After obtaining the certificate issuance request, the CA shall determine its validity, and issue the certificate after approving the application. For the issue of SSL Global Server Certificate, before applying for SCT data, the CA performs pre-issuance linting tools. If an error or warning is found, the issuance is held up for manual review to prevent the issuance of certificates that violate Baseline Requirements. The issuance of the certificate means that the CA has approved the certificate application completely and formally.

4.3.2 电子认证服务机构和注册机构对订户的通告 Notifications to the Subscriber by the CA of Issuance of Certificate

CA 机构通过注册机构告知证书订户证书的签发结果和获取证书的方式，可通过面对面、电子邮件、网络下载，或 CA 机构认为其他安全可行的方式告知订户。

The CA shall inform the subscriber through the face-to-face, e-mail, network download, or other means that the CA considers safe and feasible through the RA of the issuance of the subscriber certificate and the way to obtain.

4.4证书接受 Certificate Acceptance

4.4.1 构成接受证书的行为 Conduct Constituting Certificate Acceptance

证书签发完成后，订户通过 CA 机构所通告的方式获取证书，在订户发生以下任意一种行为后，CA 机构认为订户接受了证书：

1) 订户下载或安装了证书；

2) 本 CA 机构在订户的允许下，代替订户下载证书，并把证书通过邮件方式发送给订户；

3) 在本 CA 机构将证书获取通知发送给订户后，在约定的时间内订户未表示拒绝。

After the certificate is issued, the subscriber obtains the certificate through the method announced by the CA. After the subscriber has any of the following actions, the CA considers that the subscriber has accepted the certificate:

1) The subscriber has downloaded or installed the certificate;

2) The CA, with the permission of the subscriber, downloads the certificate in place of the subscriber and sends the certificate to the subscriber by email;

3) After the CA sends the certificate acquisition notice to the subscriber, the

subscriber does not refuse within the agreed time.

4.4.2 电子认证服务机构对证书的发布 Publication of the Certificate By the CA

在全球服务器证书签发之前，CA 机构根据 Google 的 CT 策略（https://github.com/chromium/ct-policy），将预证书提交至不少于 3 个合格的 CT 服务器中。CA 机构在签发证书后，将证书发给订户视为证书的发布。

Prior to the issuance of a Global Server Certificate, the CA submitted the pre-certificate to no less than three qualified CT servers based on Google's CT policy (https://github.com/chromium/ct-policy). After issuing the certificate, the CA sends the certificate to the subscriber as the publication of the certificate.

4.4.3 电子认证服务机构对其他实体的通告 Notification of Certificate Issuance By the CA to Other Entities

CA 机构不对其他实体进行通告，其他实体可以在信息库上自行查询。

The CA does not notify other entities, and other entities can make their own queries on the repository.

4.5密钥对和证书的使用 Key Pair and Certificate Usage

4.5.1 订户私钥和证书的使用 Subscriber Private Key and Certificate Usage

订户在提交了证书申请并接受了 CA 机构所签发的证书后，均视为已经同意遵守与 CA 机构、依赖方有关的权利和义务的条款。

The actions of submitting a certificate application and accepting the certificate issued by the CA shall be deemed the subscriber has agreed to abide by the terms and rights of the CA and the relying party.

订户只能在适用的法律、本 CPS 以及订户协议指定的应用范围内使用私钥

和证书，并且在证书到期或被撤销之后，订户必须停止使用该证书对应的私钥。

The subscriber shall only use the private key and certificate within the application scope specified by applicable law, this CPS, and subscriber agreement, and stop using the private key corresponding to the certificate after the certificate expires or is revoked.

对于 SSL/TLS 证书，订户有责任和义务保证只在证书列出的主题别名对应的服务器中部署证书。

For SSL/TLS certificates, the subscriber has the responsibility and obligation to ensure that the certificate is only deployed on the server corresponding to the Subject Alternative Name listed in the certificate.

4.5.2 依赖方公钥和证书的使用 Relying Party Public Key and Certificate Usage

依赖方只能在恰当的应用范围内依赖于证书，并且与证书要求相一致（如密钥用途扩展等）。依赖方获得对方的证书和公钥后，可以通过查看对方的证书了解对方的身份，并通过公钥验证对方电子签名的真实性。在验证电子签名的真实性时，依赖方应准确知道被签名的数据内容。

The relying party shall only rely on the certificate within the appropriate application scope and be consistent with the certificate requirements (such as key usage extensions, etc.). After the relying party obtains the certificate and public key of the other party, it can check the identity of the other party by checking the certificate, and verify the authenticity of its electronic signature through the public key. When verifying the authenticity of an electronic signature, the relying party shall know exactly the data being signed.

依赖方应验证证书的有效性，包括:

a) 用 CA 机构的证书验证证书中的签名，确认该证书是依赖方所信任的 CA 机构签发的，并且证书的内容没有被篡改。

b) 检验证书的有效期，确认该证书在有效期之内。

c) 通过查询 CRL 或 OCSP，确认该证书没有被注销。

The relying party shall verify the validity of the certificate, including:

a) Verify the signature in the certificate using the certificate of the CA, confirm that the certificate is issued by the CA that the relying party trusts, and the content of the certificate has not been tampered with.

b) Verify the validity of the certificate and confirm that the certificate is valid.

c) Confirm that the certificate has not been revoked by querying the CRL or OCSP.

在验证电子签名时，依赖方应准确知道什么数据已被签名。在公钥密码标准里，标准的签名信息格式被用来准确表示被签名的数据。

When verifying an electronic signature, the relying party shall know exactly what data has been signed. In the public key cryptography standard, the standard signature information format is used to accurately represent the signed data.

4.6证书更新 Certificate Renewal

4.6.1 证书更新的情形 Circumstance for Certificate Renewal

证书更新指在不改变证书中订户的公钥或其他任何信息的情况下，为订户签发一张新证书。本 CA 机构推荐订户优先选用证书密钥更新服务，详见本 CPS 第 4.7 节。

The Certificate renewal refers to the issuance of a new certificate to a subscriber without changing the subscriber's public key or any other information in the certificate. The CA recommends subscribers to use the certificate re-key service preferentially. For details, see Section 4.7 of this CPS.

订户需在证书到期前 30 天进行证书更新。证书过期后，订户必须重新申请新证书。

Subscribers are required to renew their certificate 30 days prior to the expiration of the certificate. After the certificate expires, the subscriber must re-apply for a new certificate.

CA 机构支持为 SSL 全球服务器证书、时间戳证书提供证书更新服务。

The CA supports certificate renewal services for SSL Global Server Certificates and Timestamp Certificates.

4.6.2 请求证书更新的实体 Who May Request Renewal

请求证书更新的实体为证书订户。

Certificate subscribers may request renewal.

4.6.3 证书更新请求的处理 Processing Certificate Renewal Requests

证书更新请求的处理过程包括申请验证、鉴别、签发证书。对申请的验证和鉴别须基于以下几个方面：

1. 订户的原证书存在并且由本 CA 机构签发；
2. 证书更新请求在许可期限内；
3. 基于原注册信息进行身份鉴别；
4. 若 CA 机构根据本 CPS 第 3.2 节获得的数据或证明文件的时间不超过本 CPS 第 6.3.2 节中约定的此类证书的最大有效期且该信息未发生变化，则 CA 机构可重用该数据或证明文件，对订户身份进行识别与鉴别。

The processing of certificate renewal requests includes application verification, authentication, and certificate issuance. The verification and authentication of the application must be based on the following aspects:

1. The original certificate of the subscriber exists, and it was issued by the CA;

2. The certificate renewal request is within the license period;

3. Identity authentication is based on the original registration information

4. If the time of obtaining data or certification by the CA in accordance with Section 3.2 of this CPS does not exceed the maximum validity period of such certificate as specified in Section 6.3.2 of this CPS and the information has not changed, the CA may reuse the data or supporting documents to identify and authenticate the identity of the subscriber.

在以上验证和鉴别通过后 CA 机构才可批准签发证书。

After the above verification and authentication are passed, the CA can approve the

issuance of the certificate.

在证书更新时，订户可以用原有的私钥对更新请求进行签名，CA 机构将会对用户的签名和公钥、更新请求内包含的用户信息进行正确性、合法性和唯一性的验证和鉴别。

When the certificate is renewed, the subscriber can sign the renewal request with the original private key, and the CA will verify and authenticate the correctness, legality and uniqueness of the user's signature and the public key and the user information contained in the renewal request.

订户也可以选择按照本 CPS 第 3.2 节的要求进行证书更新申请操作，重新提交身份证明材料，CA 机构在任何情况下都可将这种初始证书申请的鉴别方式作为证书更新时的鉴别处理手段。

The subscriber may also choose to perform the certificate renewal application operation in accordance with the requirements of Section 3.2 of this CPS, and re-submit the identity certification materials. The CA may, in any case, use the authentication method of the initial certificate application as the authentication processing method when the certificate is renewed.

4.6.4 颁发新证书时对订户的通告 Notification of New Certificate Issuance To Subscriber

同本 CPS 第 4.3.2 节。

The same as Section 4.3.2 of this CPS.

4.6.5 构成接受更新证书的行为 Conduct Constituting Acceptance of A Renewal Certificate

同本 CPS 第 4.4.1 节。

The same as Section 4.4.1 of this CPS.

4.6.6 电子认证服务机构对更新证书的发布 Publication of the Renewal Certificate By the CA

同本 CPS 第 4.4.2 节。

The same as Section 4.4.2 of this CPS.

4.6.7 电子认证服务机构对其他实体的通告 Notification of Certificate Issuance By the CA to Other Entities

同本 CPS 第 4.4.3 节。

The same as Section 4.4.3 of this CPS.

4.7证书密钥更新 Certificate Re-key

4.7.1 证书密钥更新的情形 Circumstance for Certificate Re-key

证书密钥更新是指订户生成新密钥并申请为新公钥签发新证书，CA 机构提供证书更新时，密钥必须同时更新。

The certificate re-key means that the subscriber generates a new key and requests to issue a new certificate for the new public key. When the CA provides the certificate renewal, the key must be renewed at the same time.

若 CA 机构根据本 CPS 第 3.2 节指定来源获得的数据或证明文件的时间不超过本 CPS 第 6.3.2 节中约定的此类证书的最大有效期且该信息未发生变化，则 CA 机构可以重用这些此前已验证的信息。此时，订户在申请证书密钥更新时无需再次提交证书申请所需材料，仅提交协助识别原证书的相应信息即可，如证书序列号、订户甄别名等，以及采用原证书对应私钥对证书密钥更新请求进行签名以便 CA 机构验证。

If the time of obtaining data or certification documents by CA from the source specified in Section 3.2 of this CPS does not exceed the maximum validity period of

such certificate as specified in Section 6.3.2 of this CPS and the information has not changed, the CA may reuse these previous validations. In this case, the subscriber does not need to submit the required materials for the certificate application again when applying for the certificate re-key. The subscriber shall only submit the corresponding information for assisting in identifying the original certificate, such as the certificate serial number, the subscriber's DN, etc., and sign the certificate re-key request using the private key corresponding to the original certificate for CA's verification.

证书密钥更新包括但不限于以下情形：

a) 当订户证书即将到期时；

b) 当订户证书私钥泄露而撤销证书时；

c) 当订户证实或怀疑其证书密钥不安全时；

d) 其它可能导致密钥更新的情形。

Certificate re-keys include, but are not limited to, the following circumstances:

a) when the subscriber certificate is about to expire;

b) when the subscriber certificate private key is compromised and the certificate is revoked;

c) when the subscriber confirms or suspects that its certificate key is unsafe;

d) other circumstances that may result in a re-key.

CA 机构支持为 SSL 全球服务器证书提供证书密钥更新服务。

The CA supports the provision of certificate re-key services for SSL Global Server Certificates.

4.7.2 请求证书公钥更新的实体 Who May Request Certification of a new public key

请求证书公钥更新的实体为证书订户。

Certificate subscriber may request certificate re-key.

4.7.3 证书密钥更新请求的处理 Processing Certificate Re-keying Requests

同本 CPS 第 3.3 节。

The same as Section 3.3 of this CPS.

4.7.4 颁发新证书时对订户的通告 Notification of New Certificate Issuance to Subscriber

同本 CPS 第 4.3.2 节。

The same as Section 4.3.2 of this CPS.

4.7.5 构成接受密钥更新证书的行为 Conduct Constituting Acceptance of A Re-keyed Certificate

同本 CPS 第 4.4.1 节。

The same as Section 4.4.1 of this CPS.

4.7.6 电子认证服务机构对密钥更新证书的发布 Publication of the Re-keyed Certificate By the CA

同本 CPS 第 4.4.2 节。

The same as Section 4.4.2 of this CPS.

4.7.7 电子认证服务机构对其他实体的通告 Notification of Certificate Issuance By the CA to Other Entities

同本 CPS 第 4.4.3 节。

The same as Section 4.4.3 of this CPS.

4.8证书变更 Certificate Modification

4.8.1 证书变更的情形 Circumstance for Certificate Modification

如订户提供的注册信息发生改变，必须向 CA 机构提出证书变更。证书变更的申请和证书申请所需的流程、条件一致。

If the registration information provided by the subscriber changes, a certificate modification must be submitted to the CA. The procedures and conditions required for the certificate modification application are the same as the certificate application.

4.8.2 请求证书变更的实体 Who May Request Certificate Modification

请求证书变更的实体为证书订户。

Certificate subscriber may request certificate modification.

4.8.3 证书变更请求的处理 Processing Certificate Modification Requests

证书变更按照初次申请证书的注册过程进行处理。

The certificate modification is processed according to the registration procedures of the initial certificate application.

4.8.4 颁发新证书时对订户的通告 Notification of New Certificate Issuance to Subscriber

同本 CPS 第 4.3.2 节。

The same as Section 4.3.2 of this CPS.

4.8.5 构成接受变更证书的行为 Conduct Constituting Acceptance of Modified Certificate

同本 CPS 第 4.4.1 节。

The same as Section 4.4.1 of this CPS.

4.8.6 电子认证服务机构对变更证书的发布 Publication of the Modified Certificate By the CA

同本 CPS 第 4.4.2 节。

The same as Section 4.4.2 of this CPS.

4.8.7 电子认证服务机构对其他实体的通告 Notification of Certificate Issuance by the CA to Other Entities

同本 CPS 第 4.4.3 节。

The same as Section 4.4.3 of this CPS.

4.9证书撤销和挂起 Certificate Revocation and Suspension

4.9.1 证书撤销的情形 Circumstances for Revocation

4.9.1.1 撤销订户证书的原因 Reasons for Revoking A Subscriber Certificate

如果出现下列任何一种或多种情况，CA 机构应在 24 小时内撤销该订户证书：

1. 订户以书面形式申请撤销数字证书；
2. 订户认为原始证书请求未经授权，且不能追溯授权行为；
3. CA 机构有证据证明，与订户证书中的公钥对应的私钥已泄露；

4. CA 机构获知已出现了经过验证的订户私钥泄露方法，该方法可基于公钥很容易地计算出订户私钥，包括但不限于 Baseline Requirements 第 6.1.1.3(5)节确定的方法；
5. CA 机构获得证据，证书中所包含的域名或 IP 地址的控制权验证已不再可靠；
6. CA 机构收到通知或以其他方式得知任何表明订户不再合法使用证书中电子邮件地址的情况。

The CA shall revoke the subscriber's 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 the CA that the original certificate request was not authorized and does not retroactively grant authorization;

3. The CA obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise;

4. The CA 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, including but not limited to those identified in Section 6.1.1.3(5) of Baseline Requirements;

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

6. The CA receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the certificate is no longer legally permitted.

如果出现下列任何一种或多种情况，CA 机构宜在 24 小时之内撤销证书，且必须在 5 天之内撤销证书：

1. 证书不再符合 Mozilla Root Store Policy 或 CA/Browser 论坛的 Baseline Requirements 中第 6.1.5 和 6.1.6 节的要求；

2. CA 机构掌握了证书被滥用的证据;
3. CA 机构获知订户未履行订户协议、使用条款中规定的一项或多项重要义务或责任;
4. CA 机构获知法律上不再认可该订户证书中使用的 FQDN 或 IP 地址。如，法院或仲裁员已撤销域名注册人使用域名的权利、域名注册人与申请人之间的相关许可或服务协议已终止或域名注册人未能续订域名等;
5. CA 机构获知订户的通配符证书已被用于验证欺诈性的下级域名;
6. CA 机构获知证书中包含的信息发生了重大变化;
7. CA 机构获知订户证书的签发未遵循 Baseline Requirements 或 CA 机构发布的 CP/CPS 的相关要求;
8. CA 机构确定或获知订户证书中包含了不准确或错误的信息;
9. CA 机构依据 Baseline Requirements 颁发证书的权利失效、被撤销或被终止，除非其继续维护 CRL/OCSP 信息库;
10. 当出现 CA 机构 CP/CPS 要求撤销证书的情形;
11. CA 机构获知已出现了经过验证的订户私钥泄露方法，或者有明确证据表明用于生成私钥的具体方法存在缺陷;
12. 当 CA 机构因某种原因终止电子认证服务，且未安排其他 CA 机构支持完成撤销证书的操作;
13. 订户被列入任何第三方钓鱼网站联盟、信用监管机构的黑名单中，或 CA 机构所在国家的监管机构禁止在订户经营所在地开展服务;
14. CA 机构履行证书服务费用催缴义务后，订户仍未缴纳;
15. 法律、行政法规规定的其他情形。

The CA should revoke the certificate within 24 hours and must revoke the certificate within 5 days if one or more of the following occurs:

1. The certificate no longer complies with the requirements of Mozilla Root Store Policy or Sections 6.1.5 and 6.1.6 of the Baseline Requirements of the CA/Browser Forum;

2. The CA obtains evidence that the certificate was misused;

3. The CA is made aware that a subscriber has violated one or more of its material obligations under the subscriber agreement or terms of use;

4. The CA 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. The CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified domain name;

6. The CA is made aware of a material change in the information contained in the certificate;

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

8. The CA determines or is made aware that any of the information appearing in the certificate is inaccurate;

9. The CA's right to issue certificates under Baseline Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;

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

11. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed;

12. The CA ceases operations for any reasons and has not made arrangements for another CA to provide revocation support for the certificate;

13. Subscribers are included in the blacklist of any third-party phishing website

alliance, credit regulator, or the regulatory body of the country where the CA is located prohibits conducting services at the place where the subscriber operates;

14. After the CA fulfills the obligation of urging certificate service fee, the subscriber still fails to pay;

15. Other circumstances as stipulated by laws and administrative regulations.

4.9.1.2 撤销中级 CA 证书的原因 Reasons for Revoking A Subordinate CA Certificate

如果出现下列任何一种或多种情况，CA 机构在 7 天内撤销中级 CA 证书：

1. CA 机构以书面形式申请撤销中级 CA 证书；
2. CA 机构认为中级 CA 证书请求未经授权，且不能追溯授权行为；
3. CA 机构有证据证明与证书中的公钥对应的中级 CA 的私钥已泄露，或不再符合 Baseline Requirements 第 6.1.5 和 6.1.6 节的要求；
4. CA 机构有证据证明证书被滥用；
5. CA 机构获知证书的签发未遵循 Baseline Requirements 或 CA 机构发布的 CP/CPS 的相关要求；
6. CA 机构确定了证书中包含有不准确或具有误导性的信息；
7. CA 机构或中级 CA 因任何原因停止运营，并未安排其他 CA 机构提供撤销证书的支持；
8. CA 机构依据 Baseline Requirements 颁发证书的权利到期、被撤销或被终止，除了已安排的继续维护 CRL/OCSP 信息库之外；
9. 当出现 CA 机构 CP/CPS 要求撤销证书的情形。

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

1. The Subordinate CA requests revocation in writing;

2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;

3. The CA obtains evidence that the subordinate CA's private key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of Baseline Requirements;

4. The CA obtains evidence that the certificate was misused;

5. The CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the Baseline Requirements or the applicable Certificate Policy or Certification Practice Statement;

6. The CA determines that any of the information appearing in the certificate is inaccurate or misleading;

7. The CA or subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;

8. The CA's or subordinate CA ' s right to issue certificates under Baseline Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP repository;

9. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement.

4.9.2 请求证书撤销的实体 Who Can Request Revocation

根据不同的情况，订户、CA 机构、注册机构可以发起撤销证书的请求。

Depending on the circumstances, the subscriber, CA, or the RA can initiate revocation.

此外，订户、依赖方、应用软件供应商和其他第三方均可提交证书问题报告，告知 CA 机构申请撤销证书的合理原因。

In addition, subscribers, relying parties, application software suppliers and other third parties may submit certificate problem reports informing the CA of reasonable cause to revoke the certificate.

4.9.3 撤销请求的流程 Procedure for Revocation Request

4.9.3.1 订户主动提出撤销申请 A Subscriber Makes An Application for Revocation on One’s Own Initiative

1. 证书撤销的申请人向 CA 机构或授权的注册机构提交《证书撤销申请表》，并注明撤销原因；
2. CA 机构或授权的注册机构根据本 CPS 第 3.4 节的要求对订户提交的撤销请求进行鉴别；如鉴证通过则进行撤销处理；
3. CA 机构执行撤销操作，订户证书撤销后，注册机构将通过电话、邮件等方式通知订户证书被撤销及被撤销的理由；若未能联络到订户，在必要的情况下，CA 机构对撤销的证书将通过网站进行公告；
4. CA 机构提供 7X24 小时的证书撤销申请服务，订户可通过以下方式申请撤销：

（1）发邮件至：sslservice@bjca.org.cn；或

（2）致电：+86 -4009197888。

若 SSL 证书订户通过 ACME API 提交证书撤销请求，CA 机构将通过验证域名控制权、证书撤销请求的数字签名等方式进行鉴别；如鉴证通过则进行撤销处理。

1.The applicant for the certificate revocation submits the Certificate Revocation Application Form to the CA or the authorized RA and indicates the reason for revocation;

2.The CA or the authorized RA shall authenticate the revocation request submitted by the subscriber in accordance with the requirements of Section 3.4 of this CPS and perform revocation operation if the request passes the authentication;

3.After the CA performs the revocation operation, and the subscriber's certificate is revoked, the RA shall notify the subscriber of certificate revocation and reasons for the revocation via telephone or email; in the case of failing to contact with the subscriber, the CA will announce the revoked certificate through the website if necessary;

4.The CA provides a 7X24 hours service for certificate revocation application, and subscribers can apply for revocation through the following ways:

(1) Send email to: sslservice@bjca.org.cn; or

(2) Call: +86 -4009197888.

If an SSL certificate subscriber submits a certificate revocation request through ACME API, the CA will authenticate it by verifying domain control rights, digital signatures of certificate revocation requests, and other methods; If the authentication is successful, it will be revoked.

CA 机构收到申请后 24 小时内处理撤销申请。

The CA shall process the revocation request within 24 hours of receiving the application.

4.9.3.2 订户被强制撤销证书 A Subscriber is Forced to Revoke A Certificate

1. 当 CA 机构有充分的理由确信出现本 CPS 第 4.9.1.1 节中会导致订户证书被强制撤销的情形时，CA 机构将通过内部流程申请撤销证书；
2. 在证书撤销后，CA 机构将通过适当的方式，包括邮件、电话等，通知最终订户证书已被撤销及被撤销的理由；若未能联络订户时，在必要的情况下，CA 机构对撤销的证书将通过网站进行公告；
3. CA 机构提供 7X24 小时的证书问题报告和处理流程；
4. 当依赖方如司法机构、应用软件提供商、防病毒机构等第三方发现证书可能存在问题，如证书滥用、私钥出现或怀疑出现泄漏、证书被用于可疑代码签名等，可及时通过以下方式进行问题报告：

   （1）发邮件至：sslservice@bjca.org.cn；或

   （2）致电：+86 -4009197888。

1. When the CA has sufficient reason to believe that situations that will cause the enforced revocation of subscriber certificates in Section 4.9.1.1 of this CPS occur, the CA will apply for the revocation of the certificate through the internal process;

2. After the certificate is revoked, and the CA will notify the subscriber of certificate revocation and the revocation reason through appropriate means, including email, telephone, etc. In the case of failing to contact with the subscriber, the CA will

announce the revoked certificate through the website if necessary;

3. The CA provides a 7X24 hours certificate problem report and processing flow;

4. When a relying party such as a judicial organization, application software provider, anti-virus agency, etc., finds that the certificate may have problems, such as certificate misuse, the occurrence or suspected occurrence of private key disclosure, certificate is used for suspicious code signature, etc., a timely problem report can be done in the following ways:

(1) Send email to: sslservice@bjca.org.cn; or
(2) Call: +86 -4009197888.

CA 机构收到报告后，在 24 小时内对该证书问题报告内容进行调查，并基于以下标准来决定是否撤销证书：

（1）所报告问题的性质；

（2）相应问题的出现次数和频率；

（3）问题报告或投诉的实体；

（4）订户对本 CA 机构 CP/CPS 和订户协议等相关规范的遵循情况；

（5）现行法律法规的遵循。

After receiving the report, the CA shall investigate the content of the certificate report within 24 hours and decide whether to revoke the certificate based on the following criteria:

(1) The nature of the reported problem;

(2) the occurrence number and frequency of the problem;

(3) The entity of the problem report or complaint;

(4) The subscriber's compliance with the relevant specifications of the CP/CPS and subscriber agreement of the CA;
(5) The compliance with current laws and regulations.

4.9.3.3 电子认证服务机构本身证书的撤销 Revocation of electronic certification service organization certificate

对于数字认证公司的根证书和中级 CA 证书，数字认证公司根据本 CPS 的规定决定是否撤销证书。

For BJCA's Root CA certificates and Subordinate CA certificates, revocation will be determined according to this CPS.

4.9.4 撤销请求宽限期 Revocation Request Grace Period

如果出现私钥泄露等事件，撤销请求必须在发现泄露或有泄露嫌疑 8 小时内提出。其他撤销原因的撤销请求必须在 48 小时内提出。

In the event of a private key compromise, etc., the revocation request must be filed within 8 hours of the discovery of a compromise or a suspected compromise. Revocation requests for other reasons must be filed within 48 hours.

4.9.5 电子认证服务机构处理撤销请求的时限 Time within which CA Must Process the Revocation Request

CA 机构接到撤销请求后将立即处理，调查与证书问题报告或证书撤销请求相关的事实和情况。CA 机构处理撤销请求的周期为 24 小时。

The CA shall process the request immediately after receiving the request for revocation, and investigate the facts and circumstances related to the certificate problem report or the certificate revocation request. The cycle of revocation request processing for a CA is 24 hours.

4.9.6 依赖方检查证书撤销的要求 Revocation Checking Requirement for Relying Parties

CA 机构每 24 小时签发一次 CRL，并将最新的 CRL 发布到目录服务器指定的位置，供请求者查询下载。

The CA shall issue a CRL every 24 hours and publish the latest CRL to the location specified by the directory server for the requester's query and download.

CRL 的结构如下：

a) 版本号(version)

b) 签名算法标识符(signature)

c) 颁发者名称(issure)

d) 本次更新(this update)

e) 下次更新(next update)

f) 用户证书序列号/撤销日期(user certificate/revocation date)

g) 签名算法(signature algorithm)

h) 签名(signature value)

The structure of the CRL is as follows:

a) version number (version)

b) signature algorithm identifier (signature)

c) issuer name (issure)

d) update for this time (this update)

e) update for next time (next update)

f) user certificate serial number / revocation date (user certificate / revocation date)

g) signature algorithm (signature algorithm)

h) signature (signature value)

在信任和使用证书前，依赖方必须使用以下两种功能之一进行所依赖证书的状态查询：

a) CRL 查询：利用证书中标识的 CRL 地址，通过 CRL 信息库查询并下载 CRL 到本地，进行证书状态的检验。

b) 在线证书状态查询(OCSP)：CA 机构提供 Get 和 Post 两种方式的 OCSP 查询服务，查询结果经过签名后，返回给请求者。

Before trusting and using a certificate, the relying party must use one of the following two functions to perform a status query of the dependent certificate:

a) CRL query: use the CRL address identified in the certificate to query and download the CRL locally through the CRL repository to check the certificate status.

b) Online Certificate Status Protocol (OCSP): The CA provides OCSP query services in both Get and Post modes. After the query results are signed, they are returned to the requester.

注意：依赖方要验证 CRL 的可靠性和完整性，确保是经 CA 机构发布并且签名的。

Note: The relying party shall verify the reliability and integrity of the CRL and ensure that it is issued and signed by the CA.

4.9.7 CRL 发布频率 CRL Issuance Frequency

CA 机构可采用实时或定期的方式发布 CRL。

The CA can publish CRLs in real time or on a regular basis.

发布 CRL 的频率根据证书策略确定，订户证书一般为 24 小时定期发布 CRL，并且订户 CRL 的有效期为 3 天。中级 CA 证书一般为每 12 个月定期发布 CRL，并且中级根 CRL 的有效期为 12 个月。在撤销中级 CA 证书后，将在 24 小时内更新 CRL。

The frequency of issuing CRLs is determined according to the Certificate Policy. The subscriber certificate CRLs are generally updated and reissued every 24 hours and are valid for 3 days (the value of the nextUpdate field exceeds the value of the thisUpdate field by 3 days). The subordinate CA certificate CRLs are generally updated and reissued every 12 months and are valid for 12 months (the value of the nextUpdate field exceeds the value of the thisUpdate field by 12 months). After the subordinate CA certificate is revoked, the CRL will be updated within 24 hours.

4.9.8 CRL 发布的最大滞后时间 Maximum Latency for CRLs

CRL 发布的最长滞后时间为 24 小时。

The maximum latency for CRL release is 24 hours.

4.9.9 在线状态查询的可用性 On-line Revocation/Status Checking Availability

CA 机构向订户和依赖方提供在线证书状态查询服务（OCSP），OCSP 响应符合 RFC6960 的要求，且将由审核其证书撤销状态的 CA 机构和 OCSP 响应器进行签名。

The CA provides the Online Certificate Status Protocol (OCSP) service to subscribers and relying parties. The OCSP response complies with RFC6960 and will be signed by the CA and OCSP responders that verify their certificate revocation status.

OCSP 响应器使用的签名证书服务器的证书与正在查询状态的证书由同一个 CA 签发，并且包含 RFC6960 所定义的类型为 id-pkix-ocsp-nocheck 的扩展项。

The certificate of signing certificate server used by the OCSP responder is issued by the same CA as the certificate being queried, and contains an extension of type id-pkix-ocsp-nocheck defined by RFC6960.

4.9.10 在线状态查询要求 On-line Revocation Checking Requirements

CA 机构提供 Get 和 Post 两种方式的 OCSP 查询服务。

The CA provides OCSP query services in both Get and Post methods.

对于订户证书，CA 机构至少每 4 天更新一次 OCSP 信息。OCSP 响应的最长有效期为 10 天。对于已经撤销的证书，立即更新 OCSP。

For the status of subscriber certificates, the CA shall update information provided via the OCSP at least every four days. OCSP responses must have a maximum expiration time of 10 days. For certificates that have been revoked, update the OCSP immediately.

对于中级 CA 证书，CA 机构至少每 12 个月更新一次 OCSP 信息。撤销中级 CA 证书后 24 小时内更新。

For the status of subordinate CA certificates, the CA shall update information provided via the OCSP at least every 12 months and within 24 hours after revoking a

subordinate CA certificate.

针对尚未签发的证书的在线证书状态查询请求，OCSP 响应不返回“good”状态。

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder shall not respond with a “good” status.

4.9.11 撤销信息的其他发布形式 Other Forms of Revocation Advertisements Available

证书撤销信息可以通过 CRL 或者 OCSP 服务获得。CA 机构不提供证书撤销信息的其他发布形式。

Certificate revocation information can be obtained through CRL or OCSP services. The CA does not provide other forms of certificate revocation information.

4.9.12 密钥损害的特别要求 Special Requirements Related to Key Compromise

除本 CPS 第 4.9.1 节中规定的情况外，当订户发现或有充分证据证明其密钥受到损害时，应主动及时向 CA 机构提出证书撤销请求。

Except as provided in Section 4.9.1 of this CPS, when a subscriber discovers or has sufficient evidence to prove that its key has been compromised, it shall voluntarily and timely submit a request for certificate revocation to the CA.

当各相关方发现私钥泄漏时，可通过本 CPS 第 4.9.3.2 节的规定向 CA 机构提交证书问题报告，使用以下方法中的一种来证明私钥泄露：

1. 提交由私钥签名并可通过公钥验证的签名文件；
2. 提交包含泄露私钥的二进制文件，包括提取私钥的方法。

When Parties discover that the private key is compromised, it can submit a certificate problem report to the CA according to section 4.9.3.2 of this CPS, and use one of the following methods to demonstrate private key compromise:
1. Submission of a signed file by the Private Key and verifiable by the Public Key;
2. Submission of binaries that contain a compromised Private Key, including the

method to extract the Private Key.

若新的用于证明私钥泄露的方法被采用，CA 机构将更新 CPS。

If the new method of demonstrate private key compromise is accepted, the CA will update the CPS.

4.9.13 证书挂起的情形 Circumstances for Suspension

不适用。

Not applicable.

4.9.14 请求证书挂起的实体 Who Can Request Suspension

不适用。

Not applicable.

4.9.15 挂起请求的流程 Procedure for Suspension Request

不适用。

Not applicable.

4.9.16 挂起的期限限制 Limits on Suspension Period

不适用。

Not applicable.

4.10 证书状态服务 Certificate Status Services

4.10.1 操作特征 Operational Characteristics

证书状态可以通过 CA 机构提供的 CRL、OCSP 服务查询。

The status of the certificate can be queried through the CRL and OCSP services provided by the CA.

对于被撤销的证书，CA 机构不删除其在 CRL 中的撤销记录。

For a certificate that has been revoked, the CA does not delete its revocation record in the CRL.

CA 机构不删除 OCSP 服务器中的撤销记录。

The CA does not delete the revocation record in the OCSP server.

4.10.2 服务可用性 Service Availability

CA 机构提供 7X24 小时的证书状态查询服务，且查询响应时间不超过 10 秒。

即在网络允许的情况下，订户能够实时获得证书状态查询服务。

The CA provides a 7X24 hours certificate status query service with a query response time of no more than 10 seconds. That means, the subscriber can obtain the certificate status query service in real time when the network allows.

4.10.3 可选特征 Optional Features

根据请求者的要求，在请求者支付相关费用后，CA 机构可以提供通知服务，

当指定的证书被撤销时，CA 机构将通知该项服务的请求者。

According to the requester's requirement, after the requester pays the relevant fee, the CA can provide the notification service. When the designated certificate is revoked, the CA will notify the requester of the service.

4.11 订购结束 End of Subscription

订购结束是指当证书有效期满或证书撤销后，该证书的服务时间结束。

The end of subscription means that the service time of the certificate ends when the certificate expires or the certificate is revoked.

订购结束包含以下两种情况：

a) 证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，订

户可以终止订购；

b) 在证书有效期内，证书被撤销后，即订购结束。

The end of subscription includes the following two situations:

a) When the validity of the certificate expires, and the subscriber no longer extends

the period of use of the certificate or no longer re-applies the certificate, the subscriber can terminate the subscription;

b) After the certificate is revoked within the validity period of the certificate, the subscription is terminated.

4.12 密钥托管和恢复 Key Escrow and Recovery

4.12.1 密钥托管和恢复政策及行为 Key Escrow and Recovery Policy and Practices

本CA机构全球认证体系无密钥托管和恢复业务。为了保证订户签名私钥的安全性和唯一性，建议订户自己生成密钥并进行备份，在密钥丢失后进行恢复。

This CA's global certification system does not provide key escrow and recovery services. In order to ensure the security and uniqueness of the subscriber's signature private key, it is recommended that the subscriber generates a key and makes backup so as to recover it if the key is lost.

4.12.2 会话密钥的封装与恢复的策略与行为 Session Key Encapsulation and Recovery Policy and Practices

不适用。

Not applicable.

5. 认证机构设施、管理和操作控制 Certification Authority Management Operational, and Physical Controls

5.1物理控制 Physical Controls

5.1.1 场地位置与建筑 Site Location and Construction

a) CA 机房的建筑物和机房建设按照下列标准实施:

1) GB/T 25056-2018《信息安全技术 证书认证系统密码及其相关安全技术规范》
2) GB 50174-2017:《数据中心设计规范》
3) GB/T 2887-2011:《计算机场地通用规范》
4) GB/T 9361-2011:《计算机场地安全要求》
5) GB 6650-1986:《计算机机房用活动地板技术条件》
6) GB 50116-2013:《火灾自动报警系统设计规范》
7) GB 50034-1992:《工业企业照明设计标准》
8) GB 5054-95:《低压配电装置及线路设计规范》
9) GBJ 19-87:《采暖通风与空气调节设计规范》
10) GB 50057-2010:《建筑物防雷设计规范》
11) GBJ 79-85:《工业企业通信接地设计规范》

a) The construction of the CA's facility buildings and computer rooms is implemented in accordance with the following standards:

1) GB/T 25056-2018 *Information Security Techniques--Specifications of Cryptograph and Related Security Technology for Certificate Authentication System*

2) GB 50174-2017: *Code for Design of Data Centers*

3) GB/T 2887-2011: General Specification *for Computer Field*

4) GB/T 9361-2011: *Safety Requirements for Computer Field*

5) GB 6650-1986: *Specification for Raised Floor of Computer Room*

6) GB 50116-2013: *Code for Design of Automatic Fire Alarm System*

7) GB 50034-1992: *Industrial Enterprise Lighting Design Standard*

8) GB 5054-95: *Code for Design of Low Voltage Distribution Devices and Circuits*

9) GBJ 19-87: *Design Code for Heating, Ventilation and Air Conditioning*

10) GB 50057-2010: *Design Code for Protection of Structures Against Lightning*

11) GBJ 79-85: *Specifications for the Design of Earthing of Industrial Enterprises Communication System*

b) CA 机房实行分层访问的安全管理：

CA 机房的功能区域划分为六个层次，四个区域。

六个层次由外到里分别是：入口、办公、敏感、数据中心、屏蔽机房、保密机柜。

四个区域由外到里分别是：公共区域、DMZ 区域（非军事区）、操作区域和安全区域。

其中，入口之外的区域为公共区域，入口和办公层位于 DMZ 区，敏感层位于操作区，其他各层位于安全区。

b) Security management of hierarchical access in CA's computer rooms:

The functional area of the CA's computer rooms is divided into six layers and four areas.

The six layers from the outside to the inside are: entrance, office area, sensitive, data center, shielded room, security cabinet.

The four areas from the outside to the inside are: public area, DMZ area (demilitarized area), operation area and security area.

Among them, the area outside the entrance is a public area; the entrance and office layers are located in the DMZ area; the sensitive layer is located in the operation area; and the other layers are located in the security area.

5.1.2 物理访问控制 Physical Access

为了保证本系统的安全，采取了一定的隔离、控制、监控手段。机房的所有门都足够结实，能防止非法进入。机房通过设置门禁和侵入报警系统来重点保护机房物理安全。

In order to ensure the security of the system, certain isolation, control and monitoring methods have been adopted. All doors in the computer rooms are strong enough to prevent illegal entry. The physical security of computer rooms is protected by using access control and intrusion alarm systems.

物理访问控制包括如下几个方面：

1) 门禁系统：控制各层门的进出。工作人员需使用身份识别卡结合指纹鉴定才能进出，进出每一道门应有时间纪录和信息提示。

2) 报警系统：当发生任何非法闯入、非正常手段的开门、长时间不关门等异常情况都应触发报警系统。报警系统明确指出报警位置。

3) 监控系统：与门禁和物理侵入报警系统配合使用的还有录像监控系统，对安全区域和操作区域进行 24 小时不间断录像。所有录像资料需要保留不少于 12 个月，以备查询。

Physical access control includes the following aspects:

1) Access control system: Control the entry and exit of each door. The staff member needs to use the identification card combined with fingerprint authentication to enter and exit. There shall be time record and information prompt for each door.

2) Alarm system: The alarm system shall be triggered when any illegal intrusion occurs, for example, the door is opened by abnormal means, or the door is closed for a long time, etc. The alarm system clearly indicates the location of the alarm.

3) Monitoring system: In conjunction with the access control and physical intrusion alarm system, there is also a video monitoring system for 24 hours continuous recording of the security area and operation area. All video materials must be kept for at least 12 months for queries.

门禁和物理侵入报警系统备有 UPS，并提供至少 8 小时的不间断供电。

The access control and physical intrusion alarm system is equipped with a UPS and provides at least 8 hours of uninterrupted power supply.

5.1.3 电力与空调 Power and Air Conditioning

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统，按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备分开供电。供配电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。计算机设备专用配电柜和辅助设备配电柜独立设置。

The power supply system of the computer rooms includes power, lighting, monitoring, communication, maintenance and other power systems. According to the nature of the load, it is divided into computer equipment load and auxiliary equipment load. The computer equipment and power equipment are separately powered. The power supply and distribution system consists of power distribution cabinets, power cables, trunkings and sockets, grounding lightning protection, lighting boxes and lamps, emergency lights, lighting tubes, etc. The special power distribution cabinets and auxiliary equipment power distribution cabinets for computer equipment are set independently.

使用不间断电源（UPS）来保证供电的稳定性和可靠性。采用双电源，在单路电源损坏时，可以自动切换，维持系统正常运转。

An uninterruptible power supply (UPS) is used to ensure the stability and reliability of the power supply. With dual power supply, it can be automatically switched to maintain the normal operation of the system when the single power supply is broken down.

根据机房环境及设计规范要求，主机房和基本工作间，均设置了空气调节系统。空调系统使用中央空调，并采用独立空调作为备份。其组成包括精密空调、通风管路、新风系统。

According to the requirements of the computer room environment and design specifications, air conditioning systems are installed in both the main computer room and the basic working rooms. The air conditioning system uses central air conditioning and uses a separate air conditioner as a backup. Its components include

precision air conditioning, ventilation ducts, and fresh air systems.

CA 机房的要求参照电信设施管理的规定，而且每年对物理系统的安全性进行检查。

The requirements for the CA rooms refer to the regulations for the management of telecommunication facilities, and the security of the physical system is checked every year.

5.1.4 水患防治 Water Exposures

机房内无渗水、漏水现象，主要设备采用专用的防水插座，并采取必要措施防止下雨或水管破损，造成天花板漏水、地板渗水和空调漏水等现象。

No water seepage or water leakage is allowed in the computer room. The main devices are equipped with special waterproof sockets, and necessary measures are taken to prevent rain or water pipe damage resulting in leakage of the ceiling, water seepage on the floor and water leakage of the air conditioner.

CA 机房的系统有充分保障，能够防止水侵蚀。

The system in the CA's computer room is fully protected against water erosion.

目前机房内无上下水系统，空调间做了严格防水处理，由漏水检测系统提供（7X24 小时）实时检测。

At present, there is no water supply and drainage system in the computer room. The air conditioning room has been strictly waterproofed and the water leakage detection system provides real-time detection for 7X24 hours.

5.1.5 火灾防护 Fire Prevention and Protection

火灾预防：

1) 敏感区（物理三层）、高度敏感区域（物理四、五、六层），其建筑物的耐火等级必须符合 GBJ45《高层民用建筑设计防火规范》中规定的二级耐火等级。

2) CA 机房设施内设置火灾报警装置。在机房内、各物理区域内、活动地板下、

吊顶里、主要空调管道中及易燃物附近部位设置烟、温感探测器。

3) 敏感区及高敏区配置独立的气体灭火装置，使用七氟丙烷（HFC-227ea）等洁净气体灭火系统，备有相应的气体灭火器，非敏感区根据实际情况可配置水喷淋灭火装置。CA 机房内除对纸介质等易燃物质进行灭火外，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂。

4) 火灾自动报警、自动灭火系统避开可能招致电磁干扰的区域或设备，同时配套设置消防控制室。还设有不间断的专用消防电源和直流备用电源，并具有自动和手动两种触发装置。

5) 火灾自动灭火设施的区域内，其隔墙和门的耐火极限不低于 1 小时，吊顶的耐火极限不得低于 15 分钟。

6) 在非敏感区及敏感区的办公区域内，须设置紧急出口，紧急出口必须设有消防门，消防门符合安全要求。紧急出口门外部不能有门开启的装置，且紧急出口门须与门禁报警设备联动外，需装配独立的报警设备。

7) 紧急出口有监控设备进行实时监控，并保证紧急出口门随时可用。CA 机房采取适当的管理手段来保障非紧急避险状态下，紧急出口门不能被内部人员任意打开。

Fire prevention:

1) In the sensitive area (the third physical layer), highly sensitive area (the fourth, fifth and sixth physical layers), the fire resistance of the buildings must comply with the secondary fire rating specified in GBJ45 *Specifications for the Design of Highrise Civil Buildings - Fire Prevention*.

2) A fire alarm device is installed in the CA computer room. Smoke and temperature detectors are installed in computer rooms, in various physical areas, under the raised floors, in the suspended ceilings, in the main air-conditioning ducts, and in the vicinity of flammable materials.

3) Separate gas fire extinguishers are installed in sensitive areas and high-sensitivity

areas. Clean gas fire extinguishing systems such as heptafluoropropane (HFC-227ea) are used, and the corresponding gas fire extinguishers are available. Non-sensitive areas can be equipped with water sprinklers according to actual conditions. In addition to extinguishing the flammable substances such as paper media in the CA's computer rooms, it is forbidden to use water, dry powder or foam, etc., which are prone to secondary damage.

4) Automatic fire alarm and automatic fire extinguishing system can avoid areas or equipment that may cause electromagnetic interference, with fire control rooms being set at the same time. There is also an uninterrupted special fire power supply and DC backup power supply, with both automatic and manual triggering devices.

5) In the areas equipped with automatic fire extinguishing facilities, the fire resistance limit of the partition walls and doors shall not be less than 1 hour, and the fire resistance limit of the ceilings shall not be less than 15 minutes.

6) Emergency exits shall be provided in the office areas of non-sensitive areas and sensitive areas. Fire exit doors shall be provided for emergency exits, and fire doors shall meet safety requirements. There must be no door opening device outside the emergency exit door, and the emergency exit door must be linked with the access control alarm device, with an independent alarm device being installed.

7) Emergency exits have monitoring equipment for real-time monitoring, and the emergency exit doors shall be readily available. The CA computer room adopts appropriate management measures to ensure that the emergency exit door cannot be opened arbitrarily by internal personnel under non-emergency conditions.

灭火系统采用电动，手动，紧急启动三种方式：

1) 电动方式：防护区报警系统第一次火警确认后，发出声光警示信号，切断非消防电源（如：空调电源、照明电源等）。并送排风（烟），防火阀关闭。第二次火警确认后，经延时，同时发出气体释放信号，并发出启动电信号，送给对应的管网启动钢瓶，喷气灭火。

2) 手动方式：人员对钢瓶或药剂瓶直接开启操作。

3) 紧急启动：防护区外设有紧急启动按钮供紧急时使用。

The fire extinguishing system adopts electric, manual and emergency start modes:

1) Electric mode: After the first fire alarm is confirmed in the protection zone alarm system, an acousto-optic warning signal is sent out to cut off the non-fire power supplies (such as air conditioning power supply, lighting power supply, etc.). Air (smoke) supply and exhaust systems and the fire damper are closed. After the second

fire alarm is confirmed, the gas release signal is simultaneously sent out with the start-up electric signal after the delay, and the corresponding pipe network is started for gas fire extinguishing.

2) Manual mode: The personnel can directly open the cylinder or fire extinguishing bottle.

3) Emergency start: An emergency start button is provided outside the protection zone for emergency use.

CA 机房通过与专业防火部门协调，实施消防灭火等应急响应措施。

The CA's computer room, with the coordination of the professional fire department, can implement emergency response measures such as fire extinguishing.

5.1.6 介质存储 Media Storage

CA 机房的存储介质包括硬盘、软盘、磁带、光盘等，注意防磁、防静电干扰、防火、防水，由专人管理。

The storage medium of the CA's computer room includes hard disks, floppy disks, magnetic tapes, optical disks, etc. Special personnel shall be assigned to be responsible for the anti-magnetic and anti-static interference, fire prevention and water prevention.

5.1.7 废物处理 Waste Disposal

当 CA 机房存档的敏感数据或密钥已不再需要或存档期限已满时，应当将这些数据进行销毁。纸介质、光盘或软盘必须切碎或烧毁。如果保存在磁盘中，应多次重写覆盖磁盘的存储区域，其他介质以不可恢复原则进行相应的销毁处理。密码设备在作废处置前根据制造商提供的方法先将其初始化再进行物理销毁。

When the sensitive data or keys archived in the CA's computer room shall be destroyed when they are no longer needed or the archival period is due. Paper media, optical disks or floppy disks must be shredded or burnt. If the data is saved on a magnetic disk, multiple rewriting shall be done to cover the storage area of the disk, and other media shall be destroyed according to the unrecoverable principle. The cryptographic devices shall be initialized first and then be physically destroyed according to the method provided by the manufacturer before the disposal.

5.1.8 异地备份 Off-site Backup

CA 机构建立了同城异地容灾备份中心，机房的电子认证数据实时传输到容灾备份中心，用于容灾备份系统应急恢复。

The CA has established a disaster recovery backup center in the same city. The electronic certification data of the computer room is transmitted to the disaster recovery backup center in real time for emergency recovery of the disaster recovery backup system.

5.2程序控制 Procedural Controls

5.2.1 可信角色 Trusted Roles

电子认证服务机构、注册机构、依赖方等组织中与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，必须由可信人员担任。

Staff members associated with key and certificate lifecycle management operations in organizations such as CAs, RAs, and relying parties belong to trusted roles which must be served by trusted personnel.

可信角色包括:

1) 系统管理员

系统管理员负责对数字证书服务体系在本单位的系统进行日常管理，执行系统的日常监控，并可根据需要签发服务器证书和下级操作员证书。

2) 安全管理员

安全管理员对 CA 中心的物理、网络、系统的安全全面负责。并且拟订安全管理制度和操作流程，监督各岗位安全管理的执行情况。

3) 审计管理员

审计管理员控制、管理、使用安全审计系统，安全审计系统分布于证书管理系统的各个子系统中，负责各个子系统的运行和操作日志记录。

4) 密钥管理员

密钥管理员负责管理 CA 中心的密钥相关设备，进行 CA 中心密钥的生成、备份、恢复、销毁等操作。

5) 证书业务管理员

证书业务管理员对注册机构操作员进行管理，并对注册机构业务进行管理。

6) 专业技术人员

专业技术人员对 CA、RA 系统和运营管理系统进行开发与优化、测试与验证，并为证书订户提供证书部署等相关技术支持。

Trusted roles include:

1) System administrator

The system administrator is responsible for daily management of the digital certificate service system in the system of the unit, performing daily monitoring of the system, and issuing server certificates and subordinate operator certificates as needed.

2) Security administrator

The security administrator is fully responsible for the security of the physical, network, and system of the CA center. It also formulates security administration systems and operational procedures to monitor the implementation of security administration in each position.

3) Audit administrator

The audit administrator controls, manages and uses the security audit system. The security audit system is distributed among various subsystems of the certificate management system and is responsible for the running and operation log records of each subsystem.

4) Key administrator

The key administrator is responsible for managing the key-related devices of the CA center and performing operations such as generating, backing up, restoring, and destroying keys.

5) Certificate service administrator

The certificate service administrator manages RA's operators and RA's service.

6) Technical professionals

technical professionals develop, optimize, test and verify CA and RA's system and operation management system, and provide relevant technical support for certificate deployment for certificate subscribers.

5.2.2 每项任务需要的人数 Number of Individuals Required per Task

CA 机构制定了完善的管理策略，对关键任务的职责承担严格控制，对于敏感操作，至少有两人以上的可信角色共同完成。具体地，对密钥和加密设备的操作，需要 5 个可信人员中的 3 个共同完成；对证书签发系统后台修改、增删，或审核、签发数字证书，需至少 2 个负责证书业务管理的可信人员。

The CA has developed a sound management policy for strict control over the responsibilities of key tasks. Sensitive operations are completed by at least two or more trusted individuals together. Specifically, the operation of the key and the encryption device requires three of five trusted individuals to complete together; for backstage operations of the certificate issuing system, such as to modify, add or delete, or audit and issue the digital certificate, at least two trusted individuals responsible for certificate service management are required.

5.2.3 每个角色的识别与鉴别 Identification and Authentication for Trusted Roles

所有 CA 机构的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡和指纹识别；进入系统需要使用双因素验证机制进行身份鉴别。CA 机构将独立完整地记录其所有的操作行为。

All CA's incumbents are identified according to their roles. Access to the computer room requires access card and fingerprint identification; entering the system requires a two-factor verification mechanism for identity authentication. The CA will record all its operations independently and completely.

5.2.4 需要职责分割的角色 Roles Requiring Separation of Duties

为保证系统安全，遵循可信角色分离的原则，CA 机构进行职责分离的角色，包括但不限于证书业务受理、订户身份鉴别、订户身份鉴别审批、证书或 CRL 签发、系统工程与维护、CA 密钥管理、安全审计等。

In order to ensure system security and follow the principle of separation of trusted roles, the roles that the CA implement duty separation include, but are not limited to, certificate service acceptance, subscriber identity authentication, subscriber identity authentication approval, certificate or CRL issuance, system engineering and maintenance, CA key management, security audits, etc.

5.3人员控制 Personnel Controls

5.3.1 资格、经历和无过失要求 Qualifications, Experience and Clearance Requirements

所有的员工与数字认证公司签定保密协议。对于充当可信角色或其他重要角色的人员，必须具备的一定的资格或通过 CA 机构相关的培训和考核后方能上岗，具体要求在人事管理制度中规定。CA 机构要求充当可信角色的人员至少必须具备忠诚、可信赖及工作的热诚度、无影响 CA 机构运行的其它兼职工作、无同行业重大错误记录、无违法记录等。

All employees sign a confidentiality agreement with BJCA. For those who act as trusted roles or other important roles, they must have certain qualifications or be trained and assessed by the CA before they get into jobs. The specific requirements are stipulated in the personnel management system. The CA requires that individuals acting in a trusted role must at least have loyalty, trustworthiness, and enthusiasm for work, with no other part-time work that affects the operation of the CA, no major industry error records, no illegal records, etc.

5.3.2 背景审查程序 Background Check Procedures

CA 机构与有关的政府部门和调查机构合作，完成对 CA 机构可信任员工的

背景调查。

The background check procedures for trusted employees of the CA shall be completed by the CA cooperating with relevant government departments and investigation organizations.

所有目前的可信任员工和申请调入的可信任员工都必须书面同意对其进行背景调查。

All current trusted employees and trusted employees who apply for transfer-in shall agree in writing to accept a background check.

背景调查分为：基本调查和全面调查。

Background check is divided into basic check and comprehensive check.

基本调查包括对工作经历，职业推荐，教育，社会关系方面的调查。

The basic check includes check on work experience, career recommendation, education, and social relations.

全面调查除包含基本调查项目外还包括对犯罪记录，社会关系和社会安全方面的调查。

The comprehensive check includes check on criminal records, social relations and social security in addition to basic check items.

调查程序包括：

1) 人事部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。

2) 人事部门通过电话、信函、网络、走访、等形式对其提供的材料的真实性进行鉴定。

3) 用人部门通过现场考核、日常观察、情景考验等方式对其考察。

4) 经考核，人事部门和用人部门联合填写《可信雇员调查表》，报主管领导批准后准予上岗。

The check procedure includes:

1) The personnel department is responsible for confirming the personal data of the applicants. The following materials shall be provided: relevant valid proof such as resume, graduation certificate and degree certificate of highest education, qualification certificates, ID card, etc.

2) The personnel department identifies the authenticity of the provided materials by telephone, letter, network, interview, etc.

3) The employing department examines the applicants through on-site assessment, daily observation, and scenario testing, etc.

4) After the assessment, the personnel department and the employing department jointly fill out the Trusted Employee Check Form and report to the supervisor for approval before granting the job.

5.3.3 培训要求 Training Requirements and Procedures

CA 机构对运营人员按照其岗位和角色安排不同的培训。培训有：PKI 基础知识、CP/CPS、信息验证过程中常见威胁、CA/Browser 论坛最新发布的 Baseline Requirements、系统硬件安装与维护、系统软件运行与维护、系统安全、应用软件的运行和维护、CA 的运行管理、CA 的内部管理、政策和规定及系统备份与恢复等。对负责 EV SSL 证书和 EV 代码签名的运营人员，培训 EV 证书相关标准。

The CA shall arrange different training for operators based on their positions and roles. The training includes: basic knowledge of PKI, CP/CPS, common threats to the information verification process, Baseline Requirements newly published by CA/Browser Forum, system hardware installation and maintenance, system software operation and maintenance, system security, application software operation and maintenance, operational management of the CA, internal management of the CA , policies and regulations, and system backup and recovery, etc. Operators responsible for EV SSL certificates and EV code signing shall receive training on EV certificate-related standards.

对于运营人员，其 CA 的相关知识与技能，每年至少要总结一次并由 CA 机构组织培训与考核。技术的进步、系统功能更新或新系统的加入，都需要对相关人员进行培训并考核。

For operators, the relevant knowledge and skills of CA shall be summarized at least

once a year, and the training and assessment will be organized by the CA. Advances in technology, system function updates, or the addition of new systems require training and assessment of relevant personnel.

CA 机构将员工参加培训的情况形成记录并存档，对于签发 SSL/TLS 服务器证书和代码签名证书的操作员和审核员，上岗前必须通过培训并达到 Baseline Requirements 中要求的从事该项工作所必须的技能水平。CA 机构每年至少组织一次培训与考核，确保其有足够的能力胜任该岗位。

The CA shall record and archive the employee's training. For operators and reviewers who issue SSL/TLS Server Certificates and Code Signing Certificates, they must be trained and possess the skills required for the job specified in the Baseline Requirements. The CA shall organize training and assessment at least once a year to ensure that the personnel have sufficient capacity to perform their duties.

5.3.4 再培训周期和要求 Retraining Frequency and Requirements

对于充当可信角色或其他重要角色的人员，每年至少接受 CA 机构组织的培训一次，以保证其保持完成所负责工作的技能水平。

For those who act as trusted or other important roles, they shall be trained at least once a year by the CA to ensure that they maintain the skill level that enables them to perform such duties satisfactorily.

认证策略调整、系统更新时，应对全体人员进行再培训，以适应新的变化。

When the Certification Policy is adjusted and the system is updated, all personnel shall be retrained to adapt to new changes.

5.3.5 工作岗位轮换周期和顺序 Job Rotation Frequency and Sequence

对于可替换角色，CA 机构将根据业务的安排进行工作轮换。轮换的周期和顺序，视业务的具体情况而定。

For alternative roles, the CA will implement job rotation according to the business arrangement. The frequency and sequence of rotations depend on the specifics of the business.

5.3.6 未授权行为的处罚 Sanctions for Unauthorized Actions

当 CA 机构员工被怀疑，或者已进行了未授权的操作，例如滥用权利或超出权限使用 CA 系统或进行越权操作，CA 机构得知后将立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。对情节严重的，依法追究相应责任。

When a CA employee is suspected or has performed an unauthorized operation, such as abusing rights or exceeding the authority to use the CA system or performing an unauthorized operation, the CA will immediately isolate the employee from work, and then evaluate the employee's unauthorized action, and according to the assessment results, punish the employee accordingly and take corresponding preventive measures. For serious circumstances, the corresponding responsibilities shall be investigated according to law.

5.3.7 独立合约人的要求 Independent Contractors Controls

对不属于 CA 机构的工作人员，但与本 CA 机构订户证书签发业务有关的人员等独立签约者，CA 机构的统一要求如下：

1) 人员档案备案；

2) 正规劳务公司派遣人员；

3) 具有相关业务的工作经验；

4) 必须接受 CA 组织的岗前培训和再培训要求，达到 5.3.3 要求的技能要求。

For independent contractors who are not members of the CA but are engaged in the work related to the issuance of the CA's subscriber certificates, the CA's unified requirements are specified as follows:

1) Filing of personnel files;

2) Personnel dispatched from regular labor companies;

3) Work experience with relevant business;

4) accepting the pre-job training and retraining requirements of the CA to meet the skill requirements specified by Section 5.3.3.

5.3.8 提供给员工的文档 Documentation Supplied to Personnel

为使得系统正常运行，CA 机构将向其员工提供完成其工作所必须的文档。

In order to realize proper system operation, the CA will provide its employees with the documentation necessary to complete their work.

5.4审计日志程序 Audit Logging Procedures

5.4.1 记录事件的类型 Types of Events Recorded

CA 机构对如下事件进行记录：

The CA shall record the following events:

1）CA 密钥生命周期的管理事件，包括，

- 密钥生命周期的管理事件，例如生成、备份、存储、恢复、和归档。
- 密码设备生命周期的管理事件，例如接收、使用、和销毁。

这些记录都是密钥管理员完成的手工记录。

1) CA key lifecycle management events, including,

- Key lifecycle management events, such as generation, backup, storage, recovery and archival.
- Cryptographic device lifecycle management events, such as reception, usage, and destroying.

These records are all manual records done by the key administrator.

2）CA 和订户证书生命周期的管理事件，包括，

- 证书的申请、批准、更新、撤销等。
- 成功或失败的证书操作。

这些记录由认证系统的系统日志和操作人员的手工记录组成。

2) CA and subscriber certificate lifecycles management events, including,

- Certificate application, approval, renewal, revocation, etc.
- Successful or unsuccessful certificate operations.

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

3）系统操作事件，包括，

- 系统启动和关闭。
- 系统权限的创建、删除、变更、和密码修改。

这些记录由认证系统的系统日志和操作人员的手工记录组成。

3) System operation events, including,

- System startup and shutdown.
- Creation, deletion, change and password modification of system permissions.

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

4）系统安全事件，包括，

- 成功或不成功访问 CA 系统的活动。
- 对于 CA 系统网络的非授权访问及访问企图。
- 系统崩溃，硬件故障和其他异常。
- 防火墙记录的安全事件。

这些记录由系统的自动日志和操作人员的手工记录组成。

4) System security events, including,

- Successful or unsuccessful CA system access attempts.
- Unauthorized access and access attempts to the CA system network.
- System crashes, hardware failures and other anomalies.
- Security events logged by the firewall.

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

5）CA 机构场地的工作记录，如，

- 授权人员进出。
- 非授权人员进出及陪同人。

- 场地设施的维护操作。

这些记录由系统的自动日志和操作人员的手工记录组成。

5) Work records of the CA site, for example,

- Entry and exit of authorized personnel.

- Entry and exit of non-authorized personnel and accompanying persons.

- Maintenance of site facilities.

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

日志记录一般包括如下信息：

1）事件发生的日期和时间；

2）记录的序列号；

3）记录的类型；

4）记录的来源；

5）记录事件的实体；

6）其它的事件说明信息。

Log records generally include the following elements:

1) the date and time when the event occurred;

2) the serial number of the record;

3) the type of the record;

4) the source of the record;

5) the entity of the recorded event;

6) Other event description.

5.4.2 处理日志的周期 Frequency of Processing Logs

CA 机构建有 CA 应用系统的日志收集分析系统，实时收集应用日志并归档保存。CA 机构每月进行一次日志跟踪处理，检查违反策略及其它重大事件，每月

进行发证系统日志分析。

CA has built a log collection and analysis system for the CA application system, which collects application logs in real time and archives them. The CA conducts a log tracking process every month to check for violations of policies and other major events, and conducts monthly system log analysis.

5.4.3 审计日志的保存期限 Retention Period for Audit Logs

CA 系统审计日志至少保存十年，合格审计师可按需调阅。

The CA system audit logs shall be retained for at least ten years and be available to qualified auditors upon request.

5.4.4 审计日志的保护 Protection of Audit Logs

CA 机构授权的人员才能对审查日志进行相应操作。日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、修改和删除等操作。审计日志的制作和访问进行岗位分离。

Only authorized personnel of the CA can perform corresponding operations on the audit logs. The logs are in a strict protection state and are strictly prohibit unauthorized access, reading, modification, and deletion. Post separation applies to the generation and access of the audit logs.

5.4.5 审计日志备份程序 Audit Log Backup Procedures

CA 系统审计日志备份采用数据库自身备份程序，根据记录的性质和要求，按照实时、每日、每周等策略进行备份。

The CA system audit log backup adopts the database self-backup procedures, and according to the nature and requirements of the record, it is backed up according to real-time, daily, weekly and other strategies.

5.4.6 审计收集系统 Audit Log Accumulation System

审计日志收集系统涉及：

1) 证书注册系统;

2) 证书签发系统;

3) 证书受理系统;

4) 网站和数据库系统;

5) 网络安全等其他需要审计的系统。

The audit log accumulation system involves:

1) Certificate registration system;

2) Certificate issuance system;

3) Certificate acceptance system;

4) Website and database system;

5) Other systems that require auditing, such as network security system.

CA 机构使用审计工具满足对上述系统审计的各项要求。

The CA uses audit tools to meet the requirements for auditing the above systems.

5.4.7 对导致事件实体的通告 Notification to the Event-Causing Subject

CA 机构发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，CA 机构保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

When the CA detects the attack phenomenon, it will record the attacker's actions, and trace the attacker within the scope permitted by law. The CA reserves the right to take corresponding countermeasures. According to the actions of the attacker, measures such as cutting off the services that have been opened to the attacker and submitting them to the judicial department may be taken.

CA 机构有权决定是否对导致事件的实体进行通告。

The CA has the right to decide whether to notify the event-causing subject.

5.4.8 脆弱性评估 Vulnerability Assessments

CA 机构对系统每季度进行一次漏洞扫描、每年进行一次渗透测试等脆弱性评估和识别内部和外部威胁、证书数据和管理面临的风险、以及应对这些风险的政策与程序是否完善等风险评估，以降低系统运行的风险。当 CA 机构技术架构或操作系统发生重大变更时，应进行漏洞扫描。在发现 CA 系统的重大漏洞时，CA 机构应在 4 天内完成处置。

The CA conducts vulnerability assessments on the system, such as a vulnerability scan on a quarterly basis, a penetration testing on a yearly basis, and conducts risk assessments, such as identifying internal and external threats, certificate data and management risks, and whether policies and procedures for responding to these risks are complete so as to reduce the risk of system operation. Vulnerability scanning shall be performed when there is a major change in the CA's technical architecture or operating system. When a major vulnerability in the CA system is found, it shall be handled by the CA within 4 days.

5.5记录归档 Records Archival

5.5.1 归档记录的类型 Types of Records Archived

归档记录包括所有证书申请信息、证书和证书撤销列表、与证书申请相关的信息、身份鉴别材料等。

The types of records archived include all certificate application information, certificate and certificate revocation lists, information related to certificate application, identity authentication materials, etc.

5.5.2 归档记录的保存期限 Retention Period for Archive

所有归档记录的保存期为证书失效后十年。

All archived records shall be retained for ten years after the certificate expires.

5.5.3 归档文件的保护 Protection of Archive

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能查询。CA 机构保护相关的档案内容，免遭恶劣环境的威胁，如温度、湿度和强磁力等的破坏。

The protection of archive is warranted by both physical security measures and cryptographic techniques. Only authorized personnel can queries according to a specific secure method. The CA protects related file content from threats from harsh environments such as temperature, humidity and strong magnetic forces.

5.5.4 归档文件的备份程序 Archive Backup Procedures

所有存档的文件和数据库除了保存在 CA 主机房的存储库，还在异地保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。CA 机构在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

All archived files and databases are saved in a off-site location in addition to the repository in the CA host room. Archived databases are generally physically or logically isolated, with no external information interaction. The file can only be read by authorized staff or under their supervision. The CA warrants that the deletion and modification of files and their backups are prohibited on the security mechanism.

5.5.5 记录时间戳要求 Requirements for Time-stamping of Records

所有记录都要在存档时加具体准确的时间标识以表明存档时间。系统产生的记录，用标准时间加盖时间戳。

All records must be identified by a specific time-stamping to indicate the archiving time. The records generated by the system are stamped with time-stamping in standard time.

5.5.6 归档收集系统 Archive Collection System

CA 机构有电子化的电子认证归档信息的存放系统。

The CA has an electronic storage system for electronic certification archive information.

5.5.7 获得和检验归档信息的程序 Procedures to Obtain and Verify Archive Information

由两个人分别来保留归档数据的两个拷贝，并且为了确保档案信息的准确，需要对这两个拷贝进行比较。CA 机构每年会验证归档信息的完整性。

Two copies of the archive information are separately kept by two people and need to be compared in order to ensure the accuracy of the archive information. The CA will verify the integrity of the archive information annually.

5.6电子认证服务机构密钥更替 Key Changeover

电子认证服务机构密钥更替指 CA 根证书到期和电子认证服务机构证书到期时，需要更换密钥而采取的措施。

The CA's key changeover refers to the measures taken when the CA root certificate and CA certificate expires and the key needs to be replaced.

1) CA 根密钥由加密机产生，有效期为 25 年，更替办法为：

使用旧的私钥对新的公钥及信息签名生成证书；

使用新的私钥对旧的公钥及信息签名生成证书；

使用新的私钥对新的公钥及信息签名生成证书。

通过以上 3 张证书达到密钥更换的目的，使新旧证书之间互相信任。

1) The CA root key is generated by the encryptor and is valid for 25 years. The changeover methods are:

Generate a certificate for the new public key and information signature using the old private key;

Generate a certificate for the old public key and information signature using the new private key;

Generate a certificate for the new public key and information signature using the new private key.

Through the above three methods, the purpose of key changeover can be achieved and the new and old certificates trust each other.

2) 电子认证服务机构证书到期之前，CA 机构将采取以下方式更替：

CA 机构将在 CA 证书到期前的 60 天内停止签发新的下级证书（“停止签发日期”）；

产生新的密钥对，签发新的 CA 证书；

在“停止签发日期”之后，CA 机构将采用新的 CA 密钥签发下级证书。

密钥更替时直接把当前 CA 证书撤销，签发到 CRL 并发布，然后签发一个新的 CA 证书，通过证书库和 LDAP 方式下发给证书应用系统。

2) Before the CA certificate expires, the CA will adopt the following methods for changeover:

The CA will stop issuing new subordinate certificates within 60 days before the expiration of the CA certificate ("Issuance Stop Date") ;

Generate a new key pair and issue a new CA certificate;

After the “Issuance Stop Date”, the CA will issue a subordinate certificate with the new CA key.

When the key is replaced, the current CA certificate is directly revoked, issued to the CRL and published, and then a new CA certificate is issued, which is sent to the certificate application system through the certificate library and LDAP.

3) CA 机构将继续使用旧的私有密钥签发的 CRL，直到旧的私钥签发的最后证书到期为止。

3) The CA will continue to use the CRL issued by the old private key until the last certificate issued by the old private key expires.

5.7损害与灾难恢复 Compromise and Disaster Recovery

5.7.1 事故和损害处理程序 Incident and Compromise Handling Procedures

5.7.1.1 事件响应与灾难恢复计划 Incident Response and Disaster Recovery Plans

针对故障事件，CA 机构制定了完善的应急处理预案和灾难恢复计划，发生故障时，CA 机构将执行对应处理方案，并记录事件处理过程。

For the failure event, the CA has developed a comprehensive Incident Response Plan and a Disaster Recovery Plan. When a failure occurs, the CA will execute the corresponding handling procedures and record the process.

CA 机构每年测试、审查和更新应急处理预案和灾难恢复计划，以保证有效性。

The CA annually tests, reviews, and updates the Incident Response Plan and Disaster Recovery Plan to ensure effectiveness.

5.7.1.2 大规模证书撤销计划 Mass Revocation Plans

本 CA 机构制定了全面且可行的大规模证书撤销计划，此计划每年进行测试演练并持续完善。该计划包含明确定义、可操作且全面的程序，确保快速、一致且可靠地响应大规模证书撤销情况。本 CA 机构不公开此计划，但会提供给第三方审计人员进行审计。

The CA has established a comprehensive and feasible mass revocation plan, which undergoes annual testing and drills and is continuously improved. The plan includes clearly defined, operable, and comprehensive procedures to ensure a rapid, consistent, and reliable response to mass revocation situations. The CA does not disclose this plan publicly, but will provide it to third-party auditors for auditing.

5.7.2 计算资源、软件和/或数据的损坏 Recovery Procedures if Computing Resources, Software and/or Data Are Corrupted

CA 机构遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，CA 机构将按照灾难恢复计划实施恢复。

When the CA is attacked, the communication network resources are damaged, the computer equipment system cannot provide normal services, the software is destroyed, the database is falsified, or disaster is caused by force majeure, the CA will implement recovery according to the disaster recovery plan.

5.7.3 实体私钥损害处理程序 Recovery Procedures After Key Compromise

CA 机构应每年执行一次根密钥泄漏应急程序的演练。

The CA shall perform a drill for the root key compromise emergency procedures once a year.

当 CA 根证书被作废时，CA 机构通知订户。

The CA shall notify the subscriber when the CA's Root CA Certificate is revoked.

当 CA 的私钥被攻破或需要作废时，CA 机构根据 CA 灾难恢复计划规定的灾难恢复步骤进行操作。

When the CA's private key is compromised or needs to be revoked, the CA shall operate in accordance with the disaster recovery steps specified in the CA Disaster Recovery Plan.

当 CA 机构的根 CA 或中级 CA 出现私钥损害或者证书被作废时，将通过邮件方式通知依赖方及应用软件供应商如 Mozilla/Microsoft/Apple/Google/360 等。

When the private key of Root CA Certificate or Subordinate CA Certificate is compromised or certificate is revoked, the CA will notify the relying party and

application software supplier including Mozilla/Microsoft/Apple/Google/360, etc. through email immediately.

5.7.4 灾难后的业务连续性能力 Business Continuity Capabilities After A Disaster

针对证书系统的核心业务系统，证书签发系统和证书接口系统采用双机热备方式；对核心数据库，证书管理系统数据库采用磁盘阵列方式来确保证书系统的高可靠性和可用性。

For the core business system of the certificate system, the certificate issuance system and the certificate interface system adopt the hot standby mode; for the core database, the certificate management system database adopts the disk array mode to ensure the high reliability and availability of the certificate system.

发生自然或其它不可抗力性灾难后，CA 机构可采用远程热备站点对运营进行恢复。具体的安全措施按照 CA 灾难恢复计划实施。

After a natural disaster or other force majeure disaster occurs, the CA can use an off-site hot standby station to recover operations. Specific security measures are implemented in accordance with the CA Disaster Recovery Plan.

5.8电子认证服务机构或注册机构的终止 CA or RA Termination

因各种情况，CA 机构需要终止运营时，将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

Due to various circumstances, when a CA needs to terminate its operation, it will terminate the operation in accordance with the procedures stipulated by relevant laws, and file the archives and certificates in accordance with the requirements of relevant laws and regulations.

CA 机构在终止服务九十日前，就业务承接及其他有关事项通知有关各方，包括但不限于 CA 授权的发证机构和订户等。

The CA shall notify the parties concerned, including but not limited to the issuing

authorities authorized by the CA and subscribers, on the business undertaking and other related matters 90 days before the termination of the service.

CA 机构采用以下措施终止业务：

1) 起草 CA 终止业务声明；

2) 停止认证中心所有业务；

3) 处理加密密钥；

4) 处理和存档敏感文件；

5) 清除主机硬件；

6) 处理 CA 系统业务管理员和业务操作员；

7) 通知与 CA 终止运营相关的实体。

The CA adopts the following measures to terminate the business:

1) Draft a CA business termination statement;

2) Stop all business of the Certification Center;

3) Process the encryption key;

4) Process and archive sensitive documentation;

5) Clear the host hardware;

6) Deal with CA system business administrators and business operators;

7) Notify the entities associated with the CA's termination of operations.

根据 CA 机构与注册机构签订的运营协议终止注册机构的业务。

The business of the RA is terminated in accordance with the operating agreement signed by the CA and the RA.

5.9数据安全 Data Security

数据安全符合 CA/Browser 论坛发布的 EV Guidelines 和 Code Signing Baseline Requirements 的要求。

The data security meet the requirements of the EV Guidelines and Code Signing Baseline Requirements published by the CA/Browser Forum.

6. 认证系统技术安全控制 Technical Security Controls of Certification System

6.1密钥对的生成和安装 Key Pair Generation and Installation

6.1.1 密钥对的生成 Key Pair Generation

6.1.1.1CA 密钥对生成 CA Key Pair Generation

CA 系统和 RA 系统的密钥对是在加密机内部产生，密钥在加密机的生成应遵循 FIPS 140-2 Level 3 安全规格的相关规定。在生成 CA 密钥对时，CA 机构按照加密机密钥管理制度，执行详细的操作流程控制计划，选定并授权 5 个密钥管理员，采取五选三方式，密钥管理员凭借 USBKey 对密钥进行控制。

The key pair of the CA system and the RA system is generated inside the encryptor, and the generation of the key in the encryptor shall comply with the relevant provisions of the FIPS 140-2 Level 3 security specifications. When generating a CA key pair, the CA performs a detailed operational flow control plan according to the management system of encryptor key, selects and authorizes five key administrators, and using the method of choosing three out of five, the key administrators control the key with the USBKey.

CA 密钥生成过程需要在第三方审计人员见证下进行，并由其出具见证报告。

A third-party auditor shall witness the CA key generation process and issue a witness report.

6.1.1.2 订户密钥对生成 Subscriber Key Pair Generation

对于全球服务器证书和时间戳证书，订户的密钥对由订户自己生成并保管。

对于代码签名证书、文档签名证书，本 CA 机构允许订户通过 USBKey、加密机或受签名人控制的其他安全方式（如：符合 AATL 技术标准要求）生成密钥对。若订户选择由 CA 机构代其在 CA 机构提供的 USBKey 中生成，则生成的私钥不允许明文导出，USBKey 符合 FIPS 140-2 Level 2 或相应级别安全规格；若订

户选择在自己的安全介质中生成密钥对，安全介质应符合 FIPS 140-2 Level 2 及以上或相应级别安全规格，订户在选择这些设备前，应事先向 CA 机构咨询有关系统兼容和接受事宜。

订户负有保护私钥安全的责任与义务，并承担由此带来的法律责任。如果订户使用弱密钥申请证书，CA 机构将会拒绝该申请。除订户外的其他任何机构，不应对订户私钥进行归档。

For Global Server Certificates and Timestamp Certificates, the subscriber key pair is generated and maintained by the subscriber.
For the Code Signing Certificate and the Document Signing Certificate, the CA allows the subscriber to generate key pairs via USBKey, cryptography server, or other security methods controlled by the signer (eg: complies with the AATL Technical Requirements). If the subscriber chooses CA to represent it for the generation in the USBkey provided by the CA, the generated private key shall be encrypted, and the USBKey complies with the FIPS 140-2 Level 2 security specifications or a corresponding level; if the subscriber chooses to generate a key pair on its own secure media, the secure media shall comply with FIPS 140-2 Level 2 and above security specifications or a corresponding level. Subscribers shall consult with the CA for system compatibility and acceptance before selecting these devices.
Subscribers have the responsibility and obligation to protect the security of private keys and bear the legal liabilities arising therefrom. If a subscriber uses a weak key to apply for a certificate, the CA will reject the application. No other organization than the subscriber shall archive the subscriber's private key.

6.1.2 私钥传送给订户 Private Key Delivery to Subscriber

若 CA 机构代订户在 USBKey 内部生成私钥时，由 CA 机构将 USBKey 邮寄给订户；若由订户自行生成时，不需要将私钥传送给订户。

If the CA generates the private key inside the USBKey on behalf of the subscriber, the CA will mail the USBKey to the subscriber; If the private key is generated by the subscriber itself, it is not necessary to transmit the private key to the subscriber.

6.1.3 公钥传送给证书签发机构 Public Key Delivery to Certificate Issuer

订户或订户通过注册机构，将 PKCS#10 格式的证书签名请求信息或其它数字签名的文件包，以电子文本的方式将公钥提交给本 CA 机构签发证书。当需要通过网络传送时将使用安全套接层协议（SSL）或其他安全加密方式。

The subscriber submits the public key in electronic text by sending the certificate signature request information in PKCS#10 format or other digitally signed file package by itself or through RA to the CA to issue a certificate. Secure Sockets Layer (SSL) or other secure encryption methods will be used when it needs to be transmitted over the network.

6.1.4 电子认证服务机构公钥传送给依赖方 CA Public Key Delivery to Relying Parties

本 CA 机构的公钥包含在本 CA 机构自签发的根证书和中级 CA 证书中，依赖方可以从数字认证公司官网网址：http://www.bjca.cn，下载根证书和中级 CA 证书，从而得到 CA 的公钥。

The public key of the CA is included in the Root CA Certificate and the Subordinate CA Certificate issued by the CA. The relying party can download the Root CA Certificate and the Subordinate CA Certificate from the official website of BJCA to obtain the public key of the CA: http://www.bjca.cn.

6.1.5 密钥的长度 Algorithm Type and Key Sizes

RSA 算法的根 CA 密钥长度为 4096 位，签名算法为 sha256RSA；ECC 算法的根 CA 密钥长度为 384 位（NIST P-384），签名算法为 sha384ECDSA。

The key length of Root CA Certificate of RSA algorithm is 4096 bits, and the signature algorithm is sha256RSA; the key length of Root CA Certificate of ECC algorithm is 384 bits(NIST P-384), and the signature algorithm is sha384ECDSA.

RSA 算法的中级 CA 密钥长度为 2048 位或以上，签名算法为 sha256RSA 和 sha384RSA；ECC 算法的中级 CA 密钥长度为 256 位（NIST P-256），签名算法为 sha256ECDSA 和 sha384ECDSA。

The key length of Subordinate CA Certificate of RSA algorithm is 2048 bits or more, and the signature algorithm is sha256RSA and sha384RSA; the key length of Subordinate CA Certificate of ECC algorithm is 256 bits(NIST P-256), and the signature algorithm is sha256ECDSA and sha384ECDSA.

RSA 算法的订户证书密钥长度为 2048 位或以上，签名算法为 sha256RSA；ECC 算法的订户证书密钥长度为 256 位（NIST P-256），签名算法为 sha256ECDSA。

The key length of Subscriber Certificate of RSA algorithm is 2048 bits or more, and the signature algorithm is sha256RSA; the key length of Subscriber Certificate of ECC algorithm is 256 bits(NIST P-256), and the signature algorithm is sha256ECDSA.

CA 机构使用 certlint、x509lint 和 zlint 3 个 linting 工具检测确保算法类型及密钥长度符合 CA/Browser 论坛发布的 Baseline Requirements 的要求。

The CA use three linting tools(certlint, x509lint and zlint) to ensure that the algorithm type and key size meets the requirements of the Baseline Requirements published by the CA/Browser Forum.

6.1.6 公钥参数的生成和质量检查 Public Key Parameters Generation and Quality Checking

对于使用硬件密码模块的订户，公钥参数由符合 FIPS 140-2 Level 2 安全规格的加密设备生成；对于 CA 机构，公钥参数由符合 FIPS 140-2 Level 3 安全规格的加密设备生成，并遵从这些设备的生成规范和标准。对生成的公钥参数的质量检查标准，这些设备内置的协议、算法等均已达到足够的安全等级要求。

For subscribers using the hardware cryptographic modules, the public key parameters are generated by an encryption device that complies with the FIPS 140-2 Level 2

security specifications; for the CA, the public key parameters are generated by an encryption device that complies with the FIPS 140-2 Level 3 security specifications and comply with generating specifications and standards for these devices. For the quality checking standard of the generated public key parameters, the built-in protocols and algorithms of these devices have reached sufficient security level requirements.

CA 机构使用 certlint、x509lint 和 zlint 3 个 linting 工具检测确保公钥参数符合 CA/Browser 论坛发布的 Baseline Requirements 的要求。

The CA use three linting tools(certlint, x509lint and zlint) to ensure that the public key parameters meets the requirements of the Baseline Requirements published by the CA/Browser Forum.

6.1.7 密钥使用目的 Key Usage Purposes

根 CA 密钥仅用于签署以下证书：

1) 为根 CA 自己签发的根 CA 自签名证书；

2) 中级 CA 的证书；

3) OCSP 响应验证证书。

The Root CA Certificate key is only used to sign the following certificates:

1) Self-signed Root CA Certificates issued for the root CA itself;

2) Certificates for Subordinate CA Certificates;

3) Certificates for OCSP response verification.

订户的密钥可以用于提供安全服务，例如身份认证、信息加密和解密、不可抵赖性和信息的完整性。

The subscriber's key can be used to provide security services, such as identity authentication, information encryption and decryption, non-repudiation and information integrity.

6.2私钥保护和密码模块工程控制 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 密码模块的标准和控制 Cryptographic Module Standards and Controls

CA 机构所用的密码模块经过认证，符合 FIPS 140-2 Level 3 安全规格。

The cryptographic modules used by the CA are certified and comply with FIPS 140-2 Level 3 security specifications.

6.2.2 私钥多人控制 (m 选 n) Private Key (n out of m) Multi-person Control

CA 证书的私钥的生成、激活、更新、撤销、备份和恢复等操作采用多人控制机制，即采取 5 选 3 方式，将私钥的管理权限分散到 5 个管理员 USBKey，只有其中 3 人及以上在场并许可的情况下，插入管理员 USBKey 并输入 PIN 码，才能对私钥进行上述操作。

The generation, activation, renewal, revocation, backup and recovery of the private key of the CA certificate adopts a multi-person control mechanism, that is, adopting the method of choosing 3 out of 5 to distribute the management authority of the private key to five administrators. Only when 3 or more of them are present and permit, insert the administrator's USBKey and enter the PIN code can perform the above operations on the private key.

6.2.3 私钥托管 Private Key Escrow

CA 机构的根私钥和 CA 私钥不允许托管，订户的证书对应的私钥由自己保管。

The root private key and CA private key of the CA are not allowed to be escrowed, and the private key corresponding to the subscriber's certificate is retained by

subscriber itself.

6.2.4 私钥备份 Private Key Backup

CA 私钥备份以加密的形式保存在外部存储介质中并存放在安全区域，备份私钥的恢复采用多人控制，应由 3 人或以上密钥管理员到场方能执行恢复操作，私钥备份过程应符合本 CPS 第 5.2.2 节的要求，并在安全物理环境中执行。

The CA private key backup is stored in an encrypted form on an external storage medium and stored in a secure area. The recovery of the backup private key is controlled by multiple people. Only when 3 or more key administrators are present can perform recovery operations. Private key backup process shall comply with the requirements of Section 5.2.2 of this CPS and be performed in a secure physical environment.

CA 机构不备份订户的密钥。

The CA does not backup the subscriber's key.

6.2.5 私钥归档 Private Key Archival

CA 私钥过期后，CA 机构将对 CA 私钥归档保存至少十年。对 CA 私钥归档保存的方式为加密保存在外部存储介质中并存放在安全区域。

After the CA's private keys expires, the CA shall archive and retain the CA's private keys for no less than ten years. The way to archive the CA's private keys is to encrypt and store them in an external storage medium in a secure area.

CA 机构不对订户证书的私钥进行归档。

The CA does not archive the private key of the subscriber's certificate.

6.2.6 私钥导入、导出密码模块 Private Key Transfer into or from A Cryptographic Module

CA 私钥在硬件密码模块中产生。在需要备份或迁移 CA 私钥时，从密码模块中导出的私钥应采用密文形式并由多人控制。

The CA private key is generated in the hardware cryptographic module. When a CA private key needs to be backed up or transfered, the private key exported from a cryptographic module shall be encrypted and controlled by multiple people.

订户私钥不允许从硬件密码模块中导出，CA 机构不提供订户私钥从硬件密码模块中导出的方法。

The subscriber's private key is not allowed to be exported from a hardware cryptographic module, and the CA does not provide a method for the subscriber's private key to be exported from a hardware cryptographic module.

6.2.7 私钥在密码模块的存储 Private Key Storage on Cryptographic Module

私钥以密文的方式，在硬件密码模块中加密保存。订户私钥存储在文件证书或 USBKey 等安全介质中，使用的 USBKey 等安全介质符合 FIPS 140-2 Level 2 安全规格，CA 系统采用符合 FIPS 140-2 Level 3 安全规格的密码模块，这些设备内置的协议、算法等均已达到足够的安全等级要求。

The private key is encrypted and stored on a hardware cryptographic module. The subscriber's private key is stored in file certificate or the USBKey medium. The used USBKey conforms to the FIPS 140-2 Level 2 security specifications. The CA system uses the cryptographic module that complies with the FIPS 140-2 Level 3 security specifications. The built-in protocols and algorithms of these devices have all met sufficient security level requirements.

6.2.8 激活私钥的方法 Activating Private Keys

CA 私钥存放在硬件密码模块中，激活需要按本 CPS 第 6.2.2 节使用加密设备的管理员权限实现，具有激活私钥权限的管理员使用 USBKey 登录，启动密钥管理程序，进行激活私钥的操作，需要三名管理员以上同时在场。

The CA private key is stored on a hardware cryptographic module. The activation needs to be implemented by the administrator authority of the encryption device according to Section 6.2.2 of this CPS. The administrator who has the private key

activation authority uses the USBKey to log in, starts the key management procedure, and activates the private key. This operation requires more than three administrators to be present at the same time.

订户的私钥保存在密码模块中，订户使用密码模块口令（或 PIN 码）保护私钥。订户的私钥需要验证口令（或 PIN 码）后才能被激活和使用。

The subscriber's private key is stored on a cryptographic module, and the subscriber uses the cryptographic module password (or PIN) to protect the private key. The subscriber's private key requires a verification password (or PIN) before activation and use.

6.2.9 解除私钥激活状态的方法 Deactivating Private Keys

对于 CA 私钥，具有解除私钥激活状态权限的管理员使用含有自己的身份的 USBKey 登录，启动密钥管理程序，进行解除私钥激活状态的操作，需要三名管理员以上同时在场。

For the CA private key, the administrator who has the authority to deactivate private keys uses the USBKey with his or her identity to log in, starts the key management procedure, and performs the operation of deactivating the private key, which requires more than three administrators to be present at the same time.

对于订户私钥，订户解除私钥激活状态由其自行决定。当服务程序关闭、系统注销或系统断电后私钥进入非激活状态。

For the subscriber's private key, the subscriber shall deactivate the private key at its discretion. The private key enters an inactive state when the service procedure is shut down, the system is logged off, or the system is powered off.

6.2.10 销毁私钥的方法 Destroying Private Keys

当 CA 私钥生命周期结束后，将通过本 CPS 第 6.2.5 节的方法进行 CA 私钥归档，其他的 CA 私钥备份将被安全销毁。在 CA 私钥归档期结束后，具有销毁密钥权限的管理员，启动密钥管理程序，进行销毁密钥的操作，需要 3 名或以上管理员同时在场。

When the CA private key lifecycle ends, the CA private key will be archived using the method described in Section 6.2.5 of this CPS, and other CA private key backups will be safely destroyed. After the CA private key archive period ends, the administrator with the authority to destroy the key starts the key management procedure and destroys the key. Three or more administrators need to be present at the same time.

6.2.11 密码模块能力 Cryptographic Module Capabilities

CA 机构使用的密码模块，符合 FIPS 140-2 Level 3 安全规格，支持本 CPS 第 7.1.3 节中的算法要求。

The cryptographic module used by the CA complies with FIPS 140-2 Level 3 security specifications and supports the algorithm requirements in Section 7.1.3 of this CPS.

6.3密钥对管理的其他方面 Other Aspects of Key Pair Management

6.3.1 公钥归档 Public Key Archival

CA 机构对证书公钥进行归档，证书在数据库中存放并异地备份。

The CA archives certificates' public keys, and certificates are stored in the database and backed up off-site.

6.3.2 证书操作期和密钥对使用期限 Certificate Operational Periods and Key Pair Usage Periods

CA 证书的有效期和其对应的密钥对的有效期都是一致的。订户证书的有效期和其对应密钥对的有效期保持一致。特殊情况下，对于签名类证书，为验证在证书有效期内签名的信息，公钥可以在证书有效期限以外使用。

The validity period of the CA certificate is the same as the validity period of its corresponding key pair. The validity period of the subscriber certificate is consistent with the validity period of its corresponding key pair. In special cases, for signing certificates, the public key can be used beyond the validity period of the certificate to verify the information signed within the validity period of the certificate.

对于 CA 机构的根 CA 证书，有效期最长不超过 25 年。

The CA's Root CA Certificates have a validity period no greater than 25 years.

对于 CA 中级证书，有效期最长不超过 15 年。

The CA's Subordinate CA Certificates have a validity period no greater than 15 years.

对于 SSL 全球服务器证书，有效期最长不超过 397 天。在 2020 年 8 月 31 日之前签发的 SSL 全球服务器证书，有效期最长不超过 2 年。

The SSL Global Server Certificates have a validity period no greater than 397 days. The SSL Global Server Certificates issued before August 31, 2020 are valid for a maximum of 2 years.

对于代码签名证书，有效期最长不超过 3 年。

The Code Signing Certificates have a validity period no greater than 3 years.

对于时间戳证书，有效期最长不超过 10 年。

The Timestamp Certificates have a validity period no greater than 10 years.

对于文档签名证书，有效期最长不超过 3 年。

The Document Signing Certificates have a validity period no greater than 3 years.

6.4激活数据 Activation Data

6.4.1 激活数据的产生和安装 Activation Data Generation and Installation

为了保护私钥的安全，证书订户产生和安装激活数据必须保证安全可靠，从而避免私钥被泄漏、被偷窃、被非法使用、被篡改、或者被非法授权的披露。

In order to protect the security of the private key, the certificate subscriber shall ensure that the activation data is secure and reliable, thereby preventing the private key from being disclosed, stolen, illegally used, tampered with, or published with illegal authorization.

CA 私钥的产生遵循本 CPS 第 6.2.2 节中的要求，严格进行生成、分发和使用。

The CA private key is generated in accordance with the requirements in Section 6.2.2 of this CPS and is strictly created, distributed, and used.

订户私钥的激活数据，包括用于下载证书的口令（以邮件等形式提供）、USBKey 登录口令等，都必须在安全可靠的环境下随机产生。这些激活数据，都是通过安全可靠的方式，如离线当面递交、邮政专递等方式交给订户。对于非一次性使用的激活数据，CA 机构建议用户自行进行修改。

The activation data of the subscriber's private key, including the password (provided in the form of mail, etc.) used to download the certificate, the USBKey login password, etc., must be randomly generated in a secure and reliable environment. These activation data are delivered to subscribers using secure and reliable manners, such as offline face-to-face delivery, post courier delivery, etc. For non-disposable activation data, the CA recommends that users modify it themselves.

如果订户证书私钥的激活数据是口令，这些口令必须：

1) 至少 8 位字符或数字；

2) 至少包含一个字符和一个数字；

3) 不能包含很多相同的字符；

4) 不能和操作员的名字相同；

5) 不能包含用户名信息中的较长的子字符串。

If the activation data for the subscriber certificate's private key is a password, the password shall:

1) contain at least 8 characters or numbers;

2) contain at least one character and one number;

3) cannot contain many of the same characters;

4) cannot be the same as the operator's name;

5) cannot contain longer substrings in the username information.

6.4.2 激活数据的保护 Activation Data Protection

CA 私钥的激活数据，CA 机构按照可靠的方式将激活数据分割后由不同的可

信人员掌管。

The activation data of the CA private key is split by the CA in a reliable manner and delivered to different trusted personnel for management.

如果证书订户使用口令或 PIN 值保护私钥，订户应妥善保管好其口令或 PIN 值，并根据业务应用的需要随时进行变更，防止泄露或窃取。

If a certificate subscriber uses a password or PIN value to protect the private key, the subscriber shall keep its password or PIN value properly and make changes at any time to prevent disclosure or theft as needed by the business application.

6.4.3 激活数据的其他方面 Other Aspects of Activation Data

当订户私钥的激活数据进行传输时，需要保护激活数据在传输过程中免于丢失、偷窃、修改、泄露、或非授权使用，私钥激活数据与私钥存储介质应采用不同的传输通道分发给订户。

When the activation data of the subscriber's private key is transmitted, it is necessary to protect the data from being lost, stolen, modified, disclosed, or unauthorized use during transmission. The activation data and the storage medium of a private key shall be distributed by different transmission channels to the subscriber.

订户证书私钥的激活数据由订户自己进行保管、变更。在不需要时订户自行销毁激活数据，并确保他人无法通过残余信息、存储介质直接或间接的恢复订户私钥的激活数据。

The activation data of the subscriber certificate private key is retained and changed by the subscriber. The subscriber shall destroy the activation data on its own when it is not needed and ensure that the activation data of the subscriber's private key cannot be directly or indirectly recovered by the residual information or the storage medium.

6.5计算机安全控制 Computer Security Controls

6.5.1 特别的计算机安全技术要求 Specific Computer Security Technical Requirements

CA 系统的信息安全管理符合国家相关规定，主要安全技术和控制措施包括：采取严格的身份识别和人员访问控制、安全可信的操作系统、多层防火墙设置、防病毒软件、人员职责分权管理等。

The information security management of the CA system complies with relevant national regulations. The main security technologies and control measures include: strict identification and personnel access control, secure and trusted operating system, multi-layer firewall settings, anti-virus software, and decentralized management of personnel responsibility.

对每位拥有系统（包括 CA 系统、RA 系统）业务操作权限的可信人员实行严格的双因素验证机制，访问时同时采用用户名、口令以及数字证书双因素登录方式。

A strict two-factor authentication mechanism is implemented for each trusted person who has the business operation authority of the system (including the CA system and the RA system), i.e. to use the login mode of two factors, user name, password and digital certificate simultaneously for the access.

通过严格的安全控制手段，确保 CA 软件和数据文件的系统是安全可信的系统，不会受到未经授权的访问。

Through strict security controls, the system of CA software and data files is ensured to be a secure and trusted system without unauthorized access.

核心系统必须与其他系统物理分离，生产系统与其他系统逻辑隔离。使用防火墙阻止从内网和外网入侵生产系统网络，限制访问生产系统的活动。在需要远程进行管理时，应通过安全网关进行访问并使用双因素身份鉴别规格来识别访问者身份。

The core system must be physically separated from other systems, and the production system is logically isolated from other systems. Firewalls are used to prevent the intrusion of production system networks from intranets and extranets, and restrict access to production systems. When off-site management is required, access shall be made through the security gateway and a two-factor authentication specification shall be used to identify the accessor.

6.5.2 计算机安全评估 Computer Security Rating

CA 系统使用的涉及安全的网络设备、主机、系统软件等都属经正式验收测试合格的产品。

The network equipment, host computers, system softwares, etc., used by the CA system are all products that have passed the formal acceptance test.

6.6生命周期技术控制 Life Cycle Technical Controls

6.6.1 系统开发控制 System Development Controls

CA 机构的软件设计和开发过程遵循以下原则:

1) 制定公司内部的升级变更申请制度，并要求工作人员严格按照流程执行;

2) 制定公司内部的采购流程及管理制度;

3) 开发程序必须在开发环境进行严格测试成功后，再申请部署于生产环境;

4) 变更部署前进行有效的在线备份;

5) 第三方验证和审查;

6) 安全风险分析和可靠性设计。

The software design and development process of the CA follows the following principles:

1) Develop an application system for updates and modifications within the company and require staff to strictly follow the process;

2) Develop a procurement process and management system within the company;

3) The development procedures shall apply to be deployed in the production environment after the rigorous testing in the development environment;

4) Perform an effective online backup before changing the deployment;

5) Third party verification and checking;
6) Security risk analysis and reliability design.

6.6.2 安全管理控制 Security Management Controls

CA 系统使用严格的控制措施，所有的系统都经过严格的测试验证后才能进行安装和使用。通过对系统的维护保证操作系统、网络设置和系统配置安全。通过日志检查来检查系统和数据完整性和硬件的正常操作。

The CA system adopts strict control measures, and all systems are rigorously tested and verified before they can be installed and used. The security of operating system, network settings and system configuration are ensured through system maintenance. The system and data integrity and normal operation of the hardware are checked through log checking.

6.6.3 生命期的安全控制 Life Cycle Security Controls

整个系统从设计到实现，系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计，使用的算法和密码设备均符合相关标准，使用了基于标准的强化安全通信协议确保了通信数据的安全，在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施，整个系统安全可靠。在 CA 系统运行期间，周期性开展漏洞扫描及渗透测试，并及时消除系统安全弱点。

System security is always the key point from the design to the implementation of the entire system. The system is strictly designed according to relevant national standards. The algorithms and cryptographic devices used are in compliance with relevant standards. The standard-based enhanced secure communication protocol ensures the security of communication data. In terms of system security operation, security operation measures, such as personnel authority, system backup, key recovery, etc., are fully considered so that the whole system is secure and reliable. During the operation of the CA system, vulnerability scanning and penetration testing are periodically performed, and system security weaknesses are eliminated in time.

6.7网络的安全控制 Network Security Controls

CA 机构采用多级防火墙和网络控制系统，并且实施完善的访问控制技术。

认证系统只开放与申请证书、查询证书等相关的操作功能，供用户通过网络进行操作。

为了确保网络安全，认证系统安装部署了防火墙、入侵检测、安全审计、病毒防范系统，并且及时更新防火墙、入侵监测、安全审计、病毒防范系统的版本，以尽可能的降低来自网络的风险。

CA 机构的网络安全控制符合 CA/B Forum NCSSR。

The CA adopts the protection of multi-level firewall and network control systems and implements perfect access control technology.

Authentication system only opens the relevant operation functions with the certificate application , querying the certificate to operate by network for users.

In order to ensure network security, CA's authentication system installs firewall, intrusion detection, security auditing, virus protection system, and update the version of firewall, intrusion detection, security audits, virus protection system , as much as possible to reduce the risk from the network.

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

6.8时间戳 Time-stamping

时间戳系统提供的时间戳服务在技术实现上严格遵循国际标准时间戳协议（RFC3161），采用标准的时间戳请求、时间戳应答以及时间戳编码格式，时间源采用国家授时中心提供的标准时间。

The time-stamping service provided by the time-stamping system strictly follows the international standard timestamp protocol (RFC3161) in technical implementation, adopts standard time-stamping request, response and coding forms, and the time source adopts the standard time provided by the National Time Service Center.

7. 证书、证书撤销列表和在线证书状态协议 Certificate, CRL, and OCSP Profiles

7.1证书模板 Certificate Profile

本 CA 机构签发的证书详细格式符合 X.509 V3 格式，同时遵循 RFC5280 标准。证书结构的基本域内容参考如下表格。

The detailed format of the certificate issued by this CA conforms to the X.509 V3 format and complies with the RFC5280 standard. Please refer to the following table for the basic domain content of the certificate structure.

证书结构的基本域

域	值或值的限制
版本	X.509 证书的格式版本，值为 V3。
序列号	通过 CSPRNG 生成大于零的 80 位非序列性的唯一标识符。
签名算法	签发证书时使用的签名算法（见本 CPS 第 7.1.3 节）。
签发者 DN	签发者的甄别名，包含 CN、O、C。
有效起始日期	基于国际通用时间（UTC）和北京时间同步。
有效终止日期	基于国际通用时间（UTC）和北京时间同步; 有效期限的设置符合本 CPS 规定的限制。
主题 DN	证书持有者或实体的甄别名（见本 CPS 第 7.1.4 节）。 CA 根证书甄别名，包含 CN、O、C。 CA 中级证书甄别名，包含 CN、O、C。 订户 DV 证书甄别名，包含 CN。 订户 IV 证书甄别名，包含 CN、G、SN、L、S、C。 订户 OV 证书甄别名，包含 CN、O、L、S、C。

	订户 EV SSL 证书甄别名，包含 CN、O、streetAddress、postalCode、L、S、C、serialNumber、businessCategory、jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1)、jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)、jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)，以上证书甄别名与 CA/Browser 论坛 EV Guidelines 中第 7.1.4.2 节的要求保持一致且不包含第 7.1.4.2 节规定之外的主题属性。 订户 EV 代码签名证书甄别名，包含 CN、OU、O、businessCategory、streetAddress、L、S、C、serialNumber、jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1)、jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)、jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)，以上证书甄别名与 CA/Browser 论坛 Code Signing Baseline Requirements 中第 7.1.4.2 节的要求保持一致且不包含第 7.1.4.2 节规定之外的主题属性。
公钥	根据 RFC5280 编码，使用本 CPS 第 7.1.3 节指定的算法，密钥长度满足本 CPS 第 6.1.5 节指定的要求

Basic domain of the certificate structure

Domain	Value or value limit
Version	The format version of X.509 certificate with a value of V3.
Serial Number	An 80-bit non-sequence unique identifier greater than zero generated by CSPRNG.
Signature Algorithm	The signature algorithm used to issue certificates (see Section 7.1.3 of this CPS).
Issuer's DN	Issuer's distinguished name, including CN, O, and C.
Effective start	Based on Coordinated Universal Time (UTC), synchronized with

date	Beijing time.
Effective end date	Based on Coordinated Universal Time (UTC), synchronized with Beijing time; The validity period is set in accordance with the limits set by this CPS.
Subject DN	DN of the certificate holder or entity (see Section 7.1.4 of this CPS). DN of CA's Root CA Certificate, including CN, O, C. DN of CA's Subordinate CA Certificat, including CN, O, C. DN of subscriber DV certificate, including CN. DN of subscriber IV certificate, including CN, G, SN, L, S, C. DN of subscriber OV certificate, including CN, O, L, S, C. DN of subscriber EV SSL Certificate, including CN, O, streetAddress, postalCode, L, S, C, serialNumber, businessCategory, jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1), jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2), jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3), The above certificate Subject Distinguished Name are consistent with the requirements of Section 7.1.4.2 of the CA/Browser Forum EV Guidelines and do not include any Subject attributes except as specified in Section 7.1.4.2. DN of subscriber EV Code Signing Certificate, including CN, OU, O, businessCategory, streetAddress, L, S, C, serialNumber, jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1), jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2), jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3), The above certificate Subject Distinguished Name are consistent with the requirements of Section 7.1.4.2 of the CA/Browser Forum Code Signing Baseline Requirements and do not include any Subject attributes except as specified in Section 7.1.4.2.
Public key	According to RFC5280 encoding, using the algorithm specified in Section 7.1.3 of this CPS, the key size satisfies the requirements specified in Section 6.1.5 of this CPS.

7.1.1 版本号 Version Number(s)

CA 机构签发的证书符合 X.509 V3 版本格式。版本信息在证书版本格式一栏体现。

The certificate issued by the CA conforms to the X.509 V3 version format. The version information is indicated in the column of certificate version format.

7.1.2 证书扩展项 Certificate Content and Extensions

本 CA 机构使用 X.509 V3 版证书标准项和标准扩展项，证书扩展项遵循 RFC 5280 标准，并符合 EV Guidelines 的要求。证书内容和扩展项参考如下表格。

The CA uses the X.509 V3 certificate standard items and standard extensions. The certificate extensions comply with the RFC5280 standard and comply with the requirements of the EV Guidelines. Please refer to the following table for the certificate content and extensions.

RSA 数字证书

域	根证书	中级证书	订户证书	预证书
版本	X.509 V3	X.509 V3	X.509 V3	X.509 V3
签名算法	sha256RSA	sha256RSA 或 sha384RSA	sha256RSA	sha256RSA
密钥长度	4096bits RSA	2048bits RSA 或 4096bits RSA	2048bits RSA 或 3072bits RSA	2048bits RSA
颁发机构密钥标识符	当同一个 X.500名字用于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500名字。	当同一个 X.500名字用于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500名字。	当同一个 X.500名字用于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500名字。	当同一个 X.500名字用于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500名字。
主题密钥标识符	当同一个 X.500名字用于多个证书持有者时，用一比特字符串来唯一标识证书持有者的 X.500名字。	当同一个 X.500名字用于多个证书持有者时，用一比特字符串来唯一标识证书持有者的 X.500名字。	当同一个 X.500名字用于多个证书持有者时，用一比特字符串来唯一标识证书持有者的 X.500名字。	当同一个 X.500名字用于多个证书持有者时，用一比特字符串来唯一标识证书持有者的 X.500名字。
CRL 分发点	无	由本 CA 机构指定的 CRL 发布点。	由本 CA 机构指定的 CRL 发布点。	由本 CA 机构指定的 CRL 发布点。
授权信息访问	无	包含颁发者的 OCSP 响应地址。(accessMethod = 1.3.6.1.5.5.7.48.1) 包含颁发者证书的访问地址。(accessMethod = 1.3.6.1.5.5.7.48.2)	包含颁发者的 OCSP 响应地址。(accessMethod = 1.3.6.1.5.5.7.48.1) 包含颁发者证书的访问地址。(accessMethod = 1.3.6.1.5.5.7.48.2)	包含颁发者的 OCSP 响应地址。(accessMethod = 1.3.6.1.5.5.7.48.1) 包含颁发者证书的访问地址。(accessMethod = 1.3.6.1.5.5.7.48.2)
证书策略	无	包含颁发者指定的 policy Identifier 和 CA/Browser 论坛中保留的 Policy Identifier。包含颁发者 CA 的 CPS 发布地址。	包含颁发者指定的 policy Identifier 和 CA/Browser 论坛中保留的 Policy Identifier。包含颁发者 CA 的 CPS 发布地址。	包含颁发者指定的 policy Identifier 和 CA/Browser 论坛中保留的 Policy Identifier。包含颁发者 CA 的 CPS 发布地址。

增强型密钥用法	无	进一步指明已认证的公开密钥具体用途。DocSign 中级证书无此属性。	进一步指明已认证的公开密钥具体用途。DocSign 订户证书无此属性。	服务器身份验证 (1.3.6.1.5.5.7.3.1)
基本约束	CA 证书的基本限制扩展项中的主体类型被设为 CA。	CA 证书的基本限制扩展项中的主体类型被设为 CA。	订户证书的基本限制扩展项的主体类型设为最终实体 (End-Entity)。	订户证书的基本限制扩展项的主体类型设为最终实体 (End-Entity)。
密钥用法	指明已认证的公开密钥用于何种用途。	指明已认证的公开密钥用于何种用途。	指明已认证的公开密钥用于何种用途。	指明已认证的公开密钥用于何种用途。
预认证毒药扩展	无	无	无	该项为关键扩展项（OID: 1.3.6.1.4.1.11129.2.4.3），以确保标准 X.509 V3客户端无法验证该预证书。

RSA Digital Certificate

Domain	Root certificate	Subordinate certificate	Subscriber certificate	Precertificate
Version	X.509 V3	X.509 V3	X.509 V3	X.509 V3
Signature Algorithm	sha256RSA	sha256RSA or sha384RSA	sha256RSA	sha256RSA
Key Size	4096bits RSA	2048bits RSA or 4096bits RSA	2048bits RSA or 3072bits RSA	2048bits RSA
Issuer's Key identifier	When the same X.500 name is used for multiple CAs, a one-bit string is used to uniquely identify the issuer's X.500 name.	When the same X.500 name is used for multiple CAs, a one-bit string is used to uniquely identify the issuer's X.500 name.	When the same X.500 name is used for multiple CAs, a one-bit string is used to uniquely identify the issuer's X.500 name.	When the same X.500 name is used for multiple CAs, a one-bit string is used to uniquely identify the issuer's X.500 name.
Subject Key Identifier	When the same X.500 name is used for multiple certificate holders, a one-bit string is used to uniquely identify the certificate holder's X.500 name.	When the same X.500 name is used for multiple certificate holders, a one-bit string is used to uniquely identify the certificate holder's X.500 name.	When the same X.500 name is used for multiple certificate holders, a one-bit string is used to uniquely identify the certificate holder's X.500 name.	When the same X.500 name is used for multiple certificate holders, a one-bit string is used to uniquely identify the certificate holder's X.500 name.
CRL Distribution Point	N/A	A CRL distribution point designated by the CA.	A CRL distribution point designated by the CA.	A CRL distribution point designated by the CA.

Authorization Information Access	N/A	Contains the issuer's OCSP response address. (accessMethod = 1.3.6.1.5.5.7.48.1) Contains the access address of the issuer certificate. (accessMethod = 1.3.6.1.5.5.7.48.2)	Contains the issuer's OCSP response address. (accessMethod = 1.3.6.1.5.5.7.48.1) Contains the access address of the issuer certificate. (accessMethod = 1.3.6.1.5.5.7.48.2)	Contains the issuer's OCSP response address. (accessMethod = 1.3.6.1.5.5.7.48.1) Contains the access address of the issuer certificate. (accessMethod = 1.3.6.1.5.5.7.48.2)
Certificate Policy	N/A	Contains the policy Identifier specified by the issuer and the Policy Identifier retained in the CA/Browser forum. Contains the CPS publish address of the issuer's CA.	Contains the policy Identifier specified by the issuer and the Policy Identifier retained in the CA/Browser forum. Contains the CPS publish address of the issuer's CA.	Contains the policy Identifier specified by the issuer and the Policy Identifier retained in the CA/Browser forum. Contains the CPS publish address of the issuer's CA.
Extended Key Usage	N/A	Further indicates the specific use of the certified public key. DocSign subordinate certificates do not have this attribute.	Further indicates the specific use of the certified public key. The DocSign subscriber certificate does not have this attribute.	Server Authentication (1.3.6.1.5.5.7.3.1)
Basic Constraints	The subject type in the basic restricted extension of a CA certificate is set to CA.	The subject type in the basic restricted extension of a CA certificate is set to CA.	The subject type in the basic restricted extension of a subscriber certificate is set to end entity (End-Entity).	The subject type in the basic restricted extension of a subscriber certificate is set to end entity (End-Entity).
Key Usage	Indicates the usage of the certified public key.	Indicates the usage of the certified public key.	Indicates the usage of the certified public key.	Indicates the usage of the certified public key.
Precertificate Poison	N/A	N/A	N/A	This is a critical extension (OID: 1.3.6.1.4.1.11129.2.4.3) to ensure that a standard X.509 V3 client cannot validate the precertificate.

ECC 数字证书

域	根证书	中级证书	订户证书	预证书
版本	X.509 V3	X.509 V3	X.509 V3	X.509 V3
签名算法	sha384ECDSA	sha256ECDSA 或 sha384ECDSA	sha256ECDSA	sha256ECDSA
密钥	384bits(P-384) ECC	256bits(P-256) ECC	256bits(P-256) ECC	256bits(P-256) ECC

长度				
颁发机构密钥标识符	当同一个 X.500名字用于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500名字。	当同一个 X.500名字用于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500名字。	当同一个 X.500名字用于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500名字。	当同一个 X.500名字用于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500名字。
主题密钥标识符	当同一个 X.500名字用于多个证书持有者时，用一比特字符串来唯一标识证书持有者的 X.500名字。	当同一个 X.500名字用于多个证书持有者时，用一比特字符串来唯一标识证书持有者的 X.500名字。	当同一个 X.500名字用于多个证书持有者时，用一比特字符串来唯一标识证书持有者的 X.500名字。	当同一个 X.500名字用于多个证书持有者时，用一比特字符串来唯一标识证书持有者的 X.500名字。
CRL分发点	无	由本 CA 机构指定的 CRL 发布点。	由本 CA 机构指定的 CRL 发布点。	由本 CA 机构指定的 CRL 发布点。
授权信息访问	无	包含颁发者的 OCSP 响应地址。(accessMethod = 1.3.6.1.5.5.7.48.1) 包含颁发者证书的访问地址。(accessMethod = 1.3.6.1.5.5.7.48.2)	包含颁发者的 OCSP 响应地址。(accessMethod = 1.3.6.1.5.5.7.48.1) 包含颁发者证书的访问地址。(accessMethod = 1.3.6.1.5.5.7.48.2)	包含颁发者的 OCSP 响应地址。(accessMethod = 1.3.6.1.5.5.7.48.1) 包含颁发者证书的访问地址。(accessMethod = 1.3.6.1.5.5.7.48.2)
证书策略	无	包含颁发者指定的 policy Identifier 和 CA/Browser 论坛中保留的 Policy Identifier。包含颁发者 CA 的 CPS 发布地址。	包含颁发者指定的 policy Identifier 和 CA/Browser 论坛中保留的 Policy Identifier。包含颁发者 CA 的 CPS 发布地址。	包含颁发者指定的 policy Identifier 和 CA/Browser 论坛中保留的 Policy Identifier。包含颁发者 CA 的 CPS 发布地址。
增强型密钥用法	无	进一步指明已认证的公开密钥具体用途。	进一步指明已认证的公开密钥具体用途。	服务器身份验证 (1.3.6.1.5.5.7.3.1)
基本约束	CA 证书的基本限制扩展项中的主体类型被设为 CA。	CA 证书的基本限制扩展项中的主体类型被设为 CA。	订户证书的基本限制扩展项的主体类型设为最终实体 (End-Entity)。	订户证书的基本限制扩展项的主体类型设为最终实体 (End-Entity)。
密钥用法	指明已认证的公开密钥用于何种用途。	指明已认证的公开密钥用于何种用途。	指明已认证的公开密钥用于何种用途。	指明已认证的公开密钥用于何种用途。
预认证毒药扩展	无	无	无	该项为关键扩展项（OID: 1.3.6.1.4.1.11129.2.4.3），以确保标准 X.509 V3客户端无法验证该预证书。

ECC Digital Certificate

Domain	Root certificate	Subordinate certificate	Subscriber certificate	Precertificate
Version	X.509 V3	X.509 V3	X.509 V3	X.509 V3
Signature Algorithm	sha384ECDSA	sha256ECDSA or sha384ECDSA	sha256ECDSA	sha256ECDSA

Key Size	384bits(P-384) ECC	256bits(P-256) ECC	256bits(P-256) ECC	256bits(P-256) ECC
Issuer's Key identifier	When the same X.500 name is used for multiple CAs, a one-bit string is used to uniquely identify the issuer's X.500 name.	When the same X.500 name is used for multiple CAs, a one-bit string is used to uniquely identify the issuer's X.500 name.	When the same X.500 name is used for multiple CAs, a one-bit string is used to uniquely identify the issuer's X.500 name.	When the same X.500 name is used for multiple CAs, a one-bit string is used to uniquely identify the issuer's X.500 name.
Subject Key Identifier	When the same X.500 name is used for multiple certificate holders, a one-bit string is used to uniquely identify the certificate holder's X.500 name.	When the same X.500 name is used for multiple certificate holders, a one-bit string is used to uniquely identify the certificate holder's X.500 name.	When the same X.500 name is used for multiple certificate holders, a one-bit string is used to uniquely identify the certificate holder's X.500 name.	When the same X.500 name is used for multiple certificate holders, a one-bit string is used to uniquely identify the certificate holder's X.500 name.
CRL Distribution Point	N/A	A CRL distribution point designated by the CA.	A CRL distribution point designated by the CA.	A CRL distribution point designated by the CA.
Authorization Information Access	N/A	Contains the issuer's OCSP response address. (accessMethod = 1.3.6.1.5.5.7.48.1) Contains the access address of the issuer certificate. (accessMethod = 1.3.6.1.5.5.7.48.2)	Contains the issuer's OCSP response address. (accessMethod = 1.3.6.1.5.5.7.48.1) Contains the access address of the issuer certificate. (accessMethod = 1.3.6.1.5.5.7.48.2)	Contains the issuer's OCSP response address. (accessMethod = 1.3.6.1.5.5.7.48.1) Contains the access address of the issuer certificate. (accessMethod = 1.3.6.1.5.5.7.48.2)
Certificate Policy	N/A	Contains the policy Identifier specified by the issuer and the Policy Identifier retained in the CA/Browser forum. Contains the CPS publish address of the issuer's CA.	Contains the policy Identifier specified by the issuer and the Policy Identifier retained in the CA/Browser forum. Contains the CPS publish address of the issuer's CA.	Contains the policy Identifier specified by the issuer and the Policy Identifier retained in the CA/Browser forum. Contains the CPS publish address of the issuer's CA.
Extended Key Usage	N/A	Further indicates the specific use of the certified public key.	Further indicates the specific use of the certified public key.	Server Authentication (1.3.6.1.5.5.7.3.1)
Basic Constraints	The subject type in the basic restricted extension of a CA	The subject type in the basic restricted extension of a CA certificate is set to	The subject type in the basic restricted extension	The subject type in the basic restricted extension

	certificate is set to CA.	CA.	of a subscriber certificate is set to end entity (End-Entity).	of a subscriber certificate is set to end entity (End-Entity).
Key Usage	Indicates the usage of the certified public key.	Indicates the usage of the certified public key.	Indicates the usage of the certified public key.	Indicates the usage of the certified public key.
Precertificate Poison	N/A	N/A	N/A	This is a critical extension (OID: 1.3.6.1.4.1.11129.2.4.3) to ensure that a standard X.509 V3 client cannot validate the precertificate.

对于本 CA 机构在 2020 年 7 月 1 日之后新增的中级 CA 证书包含所有适用的增强型密钥用法。对于本 CA 机构签发的 SSL 全球服务器证书、代码签名证书、时间戳证书包含所有适用的增强型密钥用法，用于指明已认证的公开密钥具体用途。增强型密钥用法参考如下表格。

For subordinate CA certificates added by the CA after July 1, 2020, all applicable EKUs must be populated. For SSL Global Server Certificates, Code Signing Certificates and Timestamp Certificates issued by the CA, all applicable EKUs must be populated to indicate the specific purpose of the authenticated public key. Please refer to the following table for Extended Key Usage.

增强型密钥用法

订户证书	增强型密钥用法
SSL 全球服务器证书	服务器身份验证 (1.3.6.1.5.5.7.3.1)
代码签名证书	代码签名 (1.3.6.1.5.5.7.3.3)
时间戳证书	时间戳 (1.3.6.1.5.5.7.3.8)

Extended Key Usage

Subscriber certificate	Extended Key Usage
SSL Global Server Certificate	Server Authentication (1.3.6.1.5.5.7.3.1)
Code Signing Certificate	Code Signing(1.3.6.1.5.5.7.3.3)

Timestamp Certificate	Time stamp (1.3.6.1.5.5.7.3.8)

7.1.3 算法对象标识符 Algorithm Object Identifiers

7.1.3.1 主题公钥信息 SubjectPublicKeyInfo

以下要求适用于证书或预证书中的主题公钥信息字段。

The following requirements apply to the subjectPublicKeyInfo field within a Certificate or Precertificate.

1）RSA 算法

本 CA 机构使用 rsaEncryption (OID:1.2.840.113549.1.1.1) 算法标识符的 RSA 密钥，参数存在并显示 NULL，不使用其他算法来表示 RSA 密钥。

2）ECDSA 算法

本 CA 机构使用 id ecPublicKey(OID:1.2.840.10045.2.1)算法标识符的 ECDSA 密钥，必须使用 namedCurve 编码。

- P-256 的密钥 namedCurve 为 secp256r1 (OID:1.2.840.10045.3.1.7)。
- P-384 的密钥 namedCurve 为 secp384r1 (OID:1.3.132.0.34)。

1) RSA
The CA indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters MUST be present, and MUST be an explicit NULL. The CA does not use other algorithms to indicate RSA keys.
2) ECDSA
The CA indicate an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters MUST use the namedCurve encoding.
• For P-256 keys, the namedCurve MUST be secp256r1 (OID: 1.2.840.10045.3.1.7).
• For P-384 keys, the namedCurve MUST be secp384r1 (OID: 1.3.132.0.34).

7.1.3.2 签名算法标识符 Signature AlgorithmIdentifier

本 CA 机构私钥签名的所有对象都符合在签名中使用算法标识符的要求。特别是，它适用于以下所有对象和字段：

- 证书或预证书的签名算法字段。

- TBS 证书的签名字段（例如，由证书或预证书使用）。
- 证书清单的签名算法字段。
- TBS 证书清单的签名字段。
- 基本 OCSP 响应的签名算法字段。

不允许对这些字段进行其他编码。

All objects signed by the CA Private Key conform to these requirements on the use of the AlgorithmIdentifier in the 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.
No other encodings are permitted for these fields.

1）RSA 签名算法

本 CA 机构使用 SHA-256 with RSA（OID：1.2.840.113549.1.1.11）签名算法。

2）ECDSA 签名算法

本 CA 机构使用以下 ECDSA 签名算法：

- SHA-256 with ECDSA（OID：1.2.840.10045.4.3.2）；
- SHA-384 with ECDSA（OID：1.2.840.10045.4.3.3）。

1) RSA
The CA uses SHA-256 with RSA (OID: 1.2.840.113549.1.1.11) signature algorithm.
2) ECDSA
The CA uses the following ECDSA signature algorithm:
• SHA-256 with ECDSA (OID: 1.2.840.10045.4.3.2);
• SHA-384 with ECDSA (OID: 1.2.840.10045.4.3.3).

7.1.4 名称形式 Name Forms

本 CA 机构签发的证书，其名称形式的格式和内容符合 RFC5280 标准，且符

合 CA/Browser 论坛 Baseline Requirements、Code Signing Baseline Requirements 及 EV Guidelines 中 7.1.4 节的要求。

The format and content of the certificate issued by the CA conform to the RFC5280 standard, and meet the requirements of section 7.1.4 in the CA/Browser forum Baseline Requirements, Code Signing Baseline Requirements and EV Guidelines.

7.1.5 名称限制 Name Constraints

无规定。

No stipulation.

7.1.6 证书策略对象标识符 Certificate Policy Object Identifier

证书策略对象标识符同本 CPS 第 1.2 节。

The certificate policy object identifier is the same as Section 1.2 of this CPS.

7.1.7 策略限制扩展项的用法 Usage of Policy Constraints Extension

无规定。

No stipulation.

7.1.8 策略限定符的语法和语义 Policy Qualifiers Syntax and Semantics

无规定。

No stipulation.

7.1.9 关键证书策略扩展项的处理规则 Processing Semantics for the Critical Certificate Policies Extension

无规定。

No stipulation.

7.2证书撤销列表 CRL Profile

CA 机构定期签发证书撤销列表，供用户查询使用。签发的证书撤销列表符合 X.509 V2 格式，遵循 RFC5280 标准。

The CA regularly issues a CRL for users to use. The issued CRL conforms to the X.509 V2 format and complies with the RFC5280 standard.

7.2.1 版本号 Version Number(s)

CA 机构签发 X.509 V2 版本的 CRL。版本信息在证书版本格式一栏体现。

The CA issues a CRL of the X.509 V2 version. The version information is indicated in the column of certificate version format.

7.2.2 CRL 和 CRL 条目扩展项 CRL and CRL Entry Extensions

本 CA 机构的证书撤销列表（CRL）是一个带时间戳并经过数字签名的已撤销证书的列表。

The Certificate Revocation List (CRL) of this CA is a list of time-stamped and digitally signed revoked certificates.

CRL 数据定义如下：

CRL 数据	定义
CRL 的版本号	指定 CRL 的版本信息，本 CA 机构采用同 X.509 V3 证书对应的 CRL V2 版本。
签名算法	本 CA 机构采用 sha256RSA 和 sha256ECDSA 签名算法。

颁发者	指定签发机构的 DN 名。
生效时间	指定一个日期/时间值，用以表明本 CRL 发布的时间。
更新时间	指定一个日期/时间值，用以表明下一次 CRL 将要发布的时间（本标准强制使用该域）。
撤销证书列表	指定已经撤销的证书列表，含有证书的序列号和证书被撤销的日期和时间。
颁发机构密钥标识符	用来验证在 CRL 上签名的公开密钥。它能辨别同一 CA 使用的不同密钥。
CRL 条目扩展项	不使用 CRL 条目扩展项。

The CRL data is defined as follows:

CRL Data	Definition
CRL Version Number	Specifies the version information of the CRL. The CA adopts the CRL V2 version corresponding to the X.509 V3 certificate.
Signature Algorithm	The CA uses signature algorithms sha256RSA and sha256ECDSA .
Issuer	Specifies the DN name of the issuing authority.
Specifies the DN name of the issuing authority.	Specify a date/time value to indicate when this CRL was published.
Update Time	Specify a date/time value to indicate when the next CRL will be published (this standard enforces this domain).
Certificate Revocation List	Specify the list of certificates that have been revoked, including the serial number of the certificate and the date and time when the certificate was revoked.
Issuer Unique Identifier	Used to verify the public key signed on the CRL. It can identify different keys used by the same CA.
CRL Entry Extensions	CRL entry extensions are not used.

7.2.2.1CRL 发布分发点 CRL Issuing Distribution Point

本 CA 机构发布完整的 CRL，所以不使用该扩展。

This extension is not used because the CA issues a full and completeCRL.

7.3在线证书状态协议 OCSP Profile

本 CA 机构采用 IETF PKIX 工作组开发的一个在线证书状态协议（Online Certificate Status Protocol，OCSP），提供在线证书状态查询服务，签发的 OCSP 响应符合 RFC6960 标准。

The CA adopts an Online Certificate Status Protocol (OCSP) developed by the IETF PKIX working group to provide an online certificate status query service, and the issued OCSP response conforms to the RFC6960 standard.

7.3.1 版本号 Version number(s)

RFC6960 定义的 OCSP v1 版。

The OCSP v1 as defined in RFC6960.

7.3.2 OCSP 扩展项 OCSP Extensions

不使用 OCSP 扩展项。

OCSP extensions are not used.

8. 认证机构审计和其他评估 Compliance Audit and Other Assessments

8.1评估的频率或情形 Frequency or Circumstances of Assessment

除了内部审计和评估外，CA 机构还进行外部审计和评估：

1) 根据《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》规定，接受相关主管部门的评估与检查；

2) 根据国际和国内相关标准，接受第三方审计机构的 WebTrust 审计。

In addition to internal audits and assessments, the CA undergoes external audits and assessments:

1) Accept the assessment and inspection of the relevant competent authorities in accordance with the *Electronic Signature Law of the People's Republic of China*, *Measures for the Administration of Electronic Certification Services* and *Regulations on Cryptographic Management of Electronic Certification Services*;

2) Accept the WebTrust audit of third-party auditors in accordance with relevant international and domestic standards.

CA 机构进行的评估频率：

1) 每年一次接受相关主管部门根据法律法规规定，对 CA 机构的年度检查；

2) CA 机构将聘请独立的审计师事务所，每年进行一次 WebTrust 审计第三方独立审计。

Frequency of assessments by CA:

1) Accept the annual inspection of the CA by the competent authorities according to the laws and regulations once a year;

2) The CA will engage an independent audit firm to conduct a third-party independent audit for WebTrust compliance anually.

8.2评估者的资质 Identity/Qualifications of Assessor

内部审计人员的选择一般包括：CA 的安全负责人及安全管理人员；CA 业务负责人；认证系统及信息系统负责人；人事负责人；其他需要的人员。

The choice of internal auditors generally includes: CA's security officers and security managers; CA business leaders; certification system and information system managers; personnel directors; other required personnel.

CA 机构将聘请熟悉 IT 运营管理且具有多年业内经验的 WebTrust 合格审计机构，对于外部审计师的资格和技能要求如下：

1) 具有公钥基础设施技术、信息安全、信息科技和系统审计有关的第三方认证服务资质；

2) 审计师所在机构具有经许可的职业资格，且在业界享有良好声誉；

3) 具有检查系统运行性能的专业技术与工具；

4) 具有有效的 WebTrust 鉴证服务资质；

5) 具有独立审计精神，受法律法规和职业道德规范的约束。

The CA will engage a qualified WebTrust practitioner that is familiar with IT operation management with years of industry experiences. The qualifications and skills required for external auditors are as follows:

1) Have third-party certification service qualifications related to public key infrastructure technology, information security, information technology and system auditing;

2) The auditor's organization has a licensed professional qualification with a good reputation in the industry;

3) Possess professional skills and tools to check the system operating performance;

4) Possess an effective WebTrust attestation service qualification;

5) Have an independent auditing spirit and be bound by laws, regulations and professional code of ethics.

8.3评估者与被评估者之间的关系 Assessor’s Relationship to Assessed Entity

内部审计人员与本 CA 机构的系统管理员、业务管理员、业务操作员的工作岗位不能重叠。

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

外部评估者与 CA 机构之间相互独立，无任何业务、财务往来或其他足以影响评估客观性的利害关系。

The external assessor is independent of the CA, and there is no business, financial transactions or other interests between them that are sufficient to influence the objectivity of the assessment.

8.4评估内容 Topics Covered By Assessment

评估审核工作包括但不限于：

1) CA 物理环境控制是否得到充分的实施；

2) 运营工作流程与制度是否得到严格遵守；

3) 是否严格按照 CPS、业务规范和安全要求开展认证业务；

4) 日志与记录是否完整无误；

5) 密钥管理、证书生命周期管理是否符合业务规则；

6) 是否存在其他潜在安全风险。

The assessment work includes but is not limited to:

1) Whether the CA's physical environment control is fully implemented;

2) Whether the operation process and system are strictly observed.

3) Whether the certification business is carried out in strict accordance with CPS, business specifications and security requirements;

4) Whether the logs and records are complete and accurate;

5) Whether key management and certificate lifecycle management conform to the practice statement;

6) Whether there is any other potential security risk.

第三方审计机构需按照 WebTrust 发布的当前有效且正在实施的各版本的审计标准，对 CA 机构进行独立审计。

The third-party auditor organization shall conduct an independent audit of the CA in accordance with the currently valid and ongoing auditing standards issued by WebTrust.

8.5对问题与不足采取的措施 Actions Taken As A Result of Deficiency

由 CA 机构管理层对审计报告进行评估，并将审计中发现的问题交由相应责任职能部门进行业务改进和完善。CA 机构将根据国际惯例和相关法律、法规迅速解决问题。

The CA's management shall assess the audit report, and the corresponding responsible functional department shall take actions for improvement and perfection of the deficiency found in the audit. The CA will quickly resolve problems in accordance with international practices and relevant laws and regulations.

8.6评估结果的传达与发布 Communication of Results

1) CA 机构内部审计结果将仅在公司内部传达；

2) 在 CA 机构接受第三方外部审计机构的评估后，CA 机构将会在公司官网 http://www.bjca.cn 公布。

3) 如 CA 机构的审计结果发现可能造成订户安全隐患的情况，则应及时向订户通报。

1) The CA internal audit results will be communicated only within the company;

2) After the CA accepts the assessment of a third-party external audit agency, it will publish the results on the company's official website http://www.bjca.cn.

3) If the audit results of the CA discover potential security concerns which may be applicable to the subscriber(s), the subscriber(s) shall be notified in time.

任何第三方向被评估实体通知评估结果或者类似的信息，都必须事先明确向

CA 机构表明通知的目的和方式，并征得 CA 机构的同意，法律另有规定的除外；CA 机构保留在这方面的法律权力。

Any third party notifying the assessed entity of the assessment resultsor similar information shall clearly indicate to the CA the purpose and manner of the notification and obtain the consent of the CA, unless otherwise provided by law; the CA retains legal power in this regard.

8.7自我评估 Self-audits

CA 机构将进行持续的自我评估，根据国际和国内相关标准和本 CPS 的规定，通过至少每年一次的内部风险评估、至少每三个月一次的抽样自我审查来严格控制服务质量。自我评估对上次审核期间末至本次审核期间初期间内的电子认证活动是否符合相关规定。抽样审查的样本数量不得少于此期间内签发证书总数的3%。

The CA will conduct ongoing self-audits and strictly control the service qualityby performing internal risk assessment on at least an annual basis and self-censorship sampling on at least a quarterly basis according to international and domestic relevant standards and this CPS. The self-audit assesses whether the electronic certification activities from the end of the last review period to the initial period of the current audit period meet the relevant regulations. The sample size of the sampling shall not be less than 3% of the total number of certificates issued during the period.

9. 法律责任和其他业务条款 Other Business and Legal Matters

9.1费用 Fees

9.1.1 证书签发和更新费用 Certificate Issuance and Renewal Fees

数字认证公司可根据提供的电子认证相关服务向证书订户收取费用，具体收费标准根据市场和管理部门的规定自行决定。CA 机构在不高于收费标准的前提下可以对证书价格进行适当调整。在订户向 CA 机构订购证书时，将提前告知证书的签发与更新费用。如果数字认证公司签署的协议中指明的价格和数字认证公司公布的价格不一致，以协议中的价格为准。

BJCA can charge the certificate subscribers according to the provided electronic certification related services. The specific charging standards are determined according to the regulations of the market and management departments. The CA can make appropriate adjustments to the certificate price without exceeding the charging standard. When a subscriber subscribes a certificate from a CA, the issuance and renewal fees of the certificate will be notified in advance. If the price specified in the agreement signed by the Certification Company is inconsistent with the price published by BJCA, the price in the agreement shall prevail.

9.1.2 证书查询费用 Certificate Access Fees

在证书有效期内，对该证书进行信息查询，CA 机构暂不收取此项费用，但保留对此项服务收费的权利。

During the validity period of the certificate, the CA does not charge fees for certificate information query for the time being, but reserves the right to charge for the service.

9.1.3 证书撤销或状态信息的查询费用 Revocation or Status Information Access Fees

CA 机构暂不收取此项费用，除非用户提出的特殊需求，需要 CA 机构支付

额外的费用，CA 机构将与用户协商收取应该收取的费用。

The CA will not charge this fee for the time being, unless the user requests special requirements which requires the CA to pay additional fees, and the CA will negotiate with the user to charge the fees that shall be charged.

9.1.4 其他服务费用 Fees for Other Services

CA 机构保留对其他服务收费的权利。CA 机构可根据请求者的要求，订制各类通知服务，具体服务费用，在与订制者签订的协议中约定。

CA reserves the right to charge for other services. The CA can customize various types of notification services according to the requirements of the applicant. The specific service fees are stipulated in the agreement with the customer.

9.1.5 退款策略 Refund Policy

在实施证书操作和签发证书的过程中，CA 机构遵守严格的操作程序和策略。除非出现 CA 机构违背了本 CPS 所规定的责任或其他重大义务的情况，订户可以要求 CA 机构撤销证书并退款，其他情况下，CA 机构对订户收取的费用均不退还。

During the implementation of certificate operations and the issuance of certificates, the CA adheres to strict operating procedures and policies. Only if the CA violates the responsibilities or other major obligations stipulated in this CPS, the subscriber may request the CA to revoke the certificate and refund. In other cases, the fee charged by the CA to the subscriber is not refundable.

完成退款后，订户如继续使用该证书，CA 机构将追究其法律责任。

After the refund is completed, the CA will pursue its legal responsibility if the subscriber continues to use the certificate.

订户应当提供符合 CA 机构要求的完整、真实、准确的证书申请信息，否则，CA 机构对此造成的损失和后果不承担任何责任。

The subscriber shall provide complete, true and accurate certificate application information in accordance with the requirements of the CA. Otherwise, the CA shall

not bear any responsibility for the losses and consequences caused thereby.

如果订户在证书服务期内退出数字证书服务体系，CA 机构将不退还剩余时间的服务费用。

If the subscriber withdraws from the digital certificate service system during the certificate service period, the CA will not refund the service fee for the remaining time.

9.2财务责任 Financial Responsibility

9.2.1 保险范围 Insurance Coverage

出现以下情形并经 CA 机构确认后，证书订户、依赖方等实体可以申请 CA 机构承担赔偿责任（法定或约定免责的除外）：

（1） CA 机构错误地将证书签发给订户以外的第三方，且导致订户或依赖方遭受损失；

（2） CA 机构发现订户提供了虚假的注册信息或资料，仍为其签发证书，并导致依赖方遭受损失；

（3） CA 机构未按鉴证要求对订户证书申请信息进行审核，并据此签发了数字，导致订户或依赖方遭受损失；

（4） CA 机构使证书私钥被破译、窃取，导致订户或依赖方遭受损失；

（5） CA 机构未能及时撤销证书，导致订户或依赖方遭受损失。

After the following circumstances have occurred and been confirmed by the CA, the certificate subscribers, relying parties and other entities may apply for the CA to bear the indemnification responsibility (except for statutory or contractual exemption):

(1) The CA incorrectly issued the certificate to a third party other than the subscriber and caused the subscriber or relying party to suffer losses;

(2) The CA finds that the subscriber has provided false registration information or information and still issues a certificate for it, causing the relying party to suffer

losses;

(3) The CA did not verify the subscriber certificate application information according to the requirements of the certification, and issued a certificate accordingly, causing the subscriber or relying party to suffer losses;

(4) The CA caused the certificate's private key to be deciphered and stolen, causing the subscriber or relying party to suffer losses;

(5) The CA failed to revoke the certificate in time, causing the subscriber or relying party to suffer losses.

CA 机构只对由于自身原因造成证书订户、依赖方的直接损失承担责任，对间接损失不承担责任。CA 机构对于任何证书或依赖方等实体的证书赔偿合计责任不得超出证书市场购买价格的 10 倍。

CA only bears the liability for the direct losses of the certificate subscriber and the relying party due to its own reasons, and bears no liability for the indirect losses. The CA's total indemnity for entities such as subscribers or relying parties shall not exceed 10 times the market purchase price of the certificate.

9.2.2 其他资产 Other Assets

CA 机构确保本公司拥有足够的财务实力以维持正常运营并保证相应义务的履行，且能够合理承担对订户及依赖方的责任。

The CA ensures that the company has sufficient financial strength to maintain normal operations and warranties the performance of its obligations, and can reasonably assume responsibility for subscribers and relying parties.

上述要求对证书订户同等适用。

The above requirements apply equally to certificate subscribers.

9.2.3 对最终实体的保险或担保 Insurance or Warranty Coverage for End-entities

CA 机构根据业务发展情况和国内保险公司的业务开展情况决定其投保策略。CA 机构通过了第三方审计公司的财务审计，为客户预留了相适配的现金资

产作为财务保证资金，当从事证书业务产生赔偿责任时用于支付相关赔偿事项。

The CA determines its insurance policies according to its business development and the business of domestic insurance companies. The CA has undergone financial auditing provided by third party auditors, and has reserved suitable cash assets for planned customers as financial guarantee for compensation arising from certification operation.

如果 CA 机构根据本 CPS 或相关法律法规的规定，以及相应的司法判定需承担赔偿和/或补偿责任的，CA 机构将按照相关法律法规规定、仲裁机构的裁定或法院的判决结果承担相应的赔偿责任。

If the CA is required to bear the indemnification and/or compensation liability according to the provisions of this CPS or relevant laws and regulations and the corresponding judicial judgment, the CA will bear the corresponding indemnification responsibilities according to the relevant laws and regulations, the arbitration institution's ruling or the court's judgment result.

9.3业务信息保密 Confidentiality of Business Information

9.3.1 保密信息范围 Scope of Confidential Information

在 CA 机构提供的电子认证服务中，保密信息包括但不限于：

1) CA 机构与订户之间的协议以及资料中未公开的内容。除法律明文规定或政府及执法机关的要求，CA 机构承诺不对外公布或透露订户证书信息以外的任何保密信息。

2) 订户私钥属于机密信息，订户应根据本 CPS 的规定进行妥善保管，如因订户个人原因导致私钥泄露而造成损失，由订户自行承担；

3) 其他由 CA 机构和 RA 保存的订户信息应视为保密，除相关法律法规或政府及执法机关的要求，不予公布。

In the electronic certification services provided by the CA, confidential information includes but is not limited to:

1) Agreement between the CA and subscribers and unpublished content in the

materials. In addition to the expressly prescribed by law or the requirements of the government and law enforcement agencies, the CA undertakes not to publish or disclose any confidential information other than the subscriber certificate information.

2) The subscriber's private key is confidential and the subscriber shall keep it properly in accordance with the stipulation of this CPS. If the private key is compromised due to the subscriber's personal reasons, the subscriber shall bear the losses;
3) Other subscriber information retained by the CA and the RA shall be considered confidential and shall not be published except as required by relevant laws and regulations or by government and law enforcement agencies.

9.3.2 不属于保密的信息 Information Not Within the Scope of Confidential Information

以下信息不属于 CA 机构认定的保密信息：

1) 与证书有关的申请流程、申请需要的手续、申请操作指南等信息；

2) 由 CA 机构签发的证书和 CRL 中的信息；

3) 由 CA 机构支持、CPS 识别的证书策略信息；

4) 提供方披露数据和信息前，已被接受方所持有的数据和信息；

5) 提供方披露数据和信息时或之后，非因接受方原因而被披露的数据和信息；

6) 有权披露的第三方披露给接受方的数据和信息；

7) 其他可通过公开渠道获取的信息。

The following information does not belong to the confidential information identified by the CA:

1) Information about the application process related to the certificate, the procedures required for the application, and the application operation guidance;

2) The certificate issued by the CA and the information in the CRL;

3) Certificate policy information supported by the CA and recognized by the CPS;

4) Data and information held by the recipient before the provider discloses the data and information;

5) Data and information that were disclosed not for the recipient's reasons when or after the provider disclosed the data and information;

6) Data and information disclosed to the recipient by third parties who have the right to disclose;

7) Other information that is available through public channels.

9.3.3 保护保密信息的责任 Responsibility to Protect Confidential Information

CA 机构通过严格的管理制度、流程和技术手段保护机密信息，包括但不限于商业机密、客户信息等。CA 机构的全体员工都将严格遵守保密条款。

The CA protects confidential information through strict management systems, processes, and technical means, including but not limited to trade secrets, customer information, etc. All employees of the CA will strictly abide by the confidentiality provisions.

CA 机构有妥善保管本 CPS 第 9.3.1 节中规定的保密信息的责任与义务。

The CA has the responsibility and obligation to keep properly keep the confidential information specified in Section 9.3.1 of this CPS.

9.4用户隐私保密 Privacy of User Information

依据相关法律、法规，CA 机构在受理客户申请证书及相关电子签名业务时，需由证书申请人及/或经办人提供相关个人信息。其中个人信息包括：姓名、联系方式、身份证号、地址和身份证（原件及/或任何形式的副本）等隐私信息。

CA 机构针对用户隐私信息提供如下保障措施。

In accordance with relevant laws and regulations, the CA needs the applicant and/or the agent to provide relevant personal information when accepting the client's certificate application and related electronic signature business. Personal information includes privacy information such as full name, contact information, ID number, address and ID card (original and/or any form of copy). The CA provides the following safeguard measures for privacy of user information.

9.4.1 隐私保密方案 Privacy Plan

CA 机构尊重证书订户个人资料的隐私权并在官网发布了个人信息保护政策，保证完全遵照国家对个人资料隐私保护的相关法律法规及有关规定。同时，CA 机构确保全体员工严格遵守安全和保密标准对个人信息给予的保密。订户选择使用 CA 机构的证书服务时，即表明已经同意接受 CA 机构的隐私保护制度。

The CA respects the privacy rights of the certificate subscriber's personal information and publishes the Personal Information Protection Policy on the official website to ensure full compliance with the relevant laws and regulations of the state regarding the privacy protection of personal information. Meanwhile, the CA ensures that all employees strictly observe the confidentiality of personal information in accordance with security and confidentiality standards. When a subscriber chooses to use a CA's certificate service, it indicates that the subscriber has agreed to accept the CA's privacy protection system.

9.4.2 作为隐私处理的信息 Information Treated as Private

CA 机构在管理和使用订户提供的相关信息时，除证书中已包含的信息以及证书状态信息外，订户的基本信息将被视为隐私处理。包括但不限于以下信息：

1) 订户的有效身份证号码，如居民身份证号码；

2) 订户的联系电话；

3) 订户的通信地址和住址；

4) 订户的银行账户。

When the CA manages and uses the relevant information provided by the subscriber, the subscriber's basic information will be treated as private, except for the information already contained in the certificate and the certificate status information. Including but not limited to the following information:

1) The valid ID number of the subscriber, such as the resident ID card number;

2) The subscriber's contact number;

3) The subscriber's communication address and residential address;

4) The subscriber’s bank account.

上述信息仅由 CA 机构使用，非经订户同意或有关法律法规、执法机关或政府根据合法的程序要求，CA 机构不会予以公开。

The above information is only used by the CA and will not be disclosed by the CA without the consent of the subscriber or by relevant laws and regulations, law enforcement agencies or the government in accordance with legal procedures.

9.4.3 不被视为隐私的信息 Information not Deemed Private

订户持有的证书信息，以及证书状态信息不被视为隐私信息。

The information of the certificate held by subscribers and certificate status information are not deemed private.

9.4.4 保护隐私的责任 Responsibility to Protecte Private Information

CA 机构有妥善保管本 CPS 第 9.4.2 节中规定的证书申请者个人信息使用、共享、管理、查阅、删改等责任与义务。

The CA has the responsibility and obligation to properly protect the use, sharing, management, checking, deletion and modification of the certificate applicant's personal information as specified in Section 9.4.2 of this CPS.

在政府或执法机关根据合法程序要求 CA 机构向特定对象公布隐私信息的情况下，CA 机构无需承担由此造成的责任。

In the case where the government or law enforcement agency requires the CA to disclose private information to a specific object in accordance with legal procedures, the CA is not liable for the resulting liability.

9.4.5 使用隐私信息的告知与同意 Notice and Consent to Use Private Information

1) 订户同意，CA 机构应采取适当的步骤保护证书订户的个人信息，应在订户协议中事先告知订户并征得订户同意；

2) 订户同意，CA 机构在业务范围内按照本 CPS 规定的隐私保护政策使用所获取的任何订户信息，如需超出约定范围及用途使用证书订户的隐私信息，应事先告知证书订户并获得同意及授权。如未获得同意及授权，CA 机构不会将订户隐私信息透露给任意第三方；

3) 订户同意，在有关法律法规、执法机关或政府根据合法的程序要求下，CA 机构向特定对象披露隐私信息时，CA 机构无需告知订户。

1) The Subscriber agrees that the CA shall take appropriate steps to protect the personal information of the certificate subscriber and shall inform the subscriber in advance in the subscriber agreement and obtain the subscriber's consent;

2) The subscriber agrees that the CA uses any subscriber information obtained in accordance with the privacy protection policy stipulated in this CPS within the scope of its business. If the subscriber's private information is used beyond the agreed scope and purpose, the CA shall inform the certificate subscriber in advance to obtain consent and authorization. Without subscribers' consent and authorization, the CA will not disclose the subscriber's private information to any third party;

3) The subscriber agrees that the CA does not need to inform the subscriber when the CA discloses the private information to a specific object under the relevant laws and regulations, or required by the law enforcement agency or the government according to the legal procedures.

9.4.6 依法律或行政程序的信息披露 Disclosure Pursuant to Judicial or Administrative Process

除非符合以下条件，CA 机构不会将订户的保密信息提供给其他第三人或第三方机构：

1) 执法机关、政府或其他相关法律法规授权的部门依据法律、法规、规章、决定、命令等提出申请；

2) 订户采用书面形式授权相关信息的披露；

3) 本 CPS 规定的其他可以披露的情形。

The CA does not provide the subscriber's confidential information to other third parties unless the following conditions are met:

1) The law enforcement agency, the government or other departments authorized by relevant laws and regulations apply according to laws, regulations, rules, decisions, orders, etc.;

2) The subscriber authorizes the disclosure of relevant information in writing;

3) Other disclosure circumstances as stipulated in this CPS.

9.4.7 其他信息披露情形 Other Information Disclosure Circumstances

如果证书订户要求 CA 机构提供某类特定客户支援服务，如资料邮寄时，CA 机构可以将不被视为订户隐私信息的相关信息，如订户的姓名和邮寄地址提供给第三方，如邮寄公司。

If the certificate subscriber requires the CA to provide certain types of customer support services, such as mailing, the CA may provide subscriber's name and mailing address and relevant information that is not deemed private to a third party, such as a mailing company.

9.5知识产权 Intellectual Property Rights

1) CA 机构享有并保留对证书及 CA 机构提供的全部软件、资料、数据等的著作权、专利申请权等全部知识产权；

2) CA 机构享有由本机构制定并发布的 CPS、CP、技术支持手册、发布的证书和 CRL 等的所有权和知识产权；

3) CA 机构官方网站上公布的一切信息均属于 CA 机构财产，未经 CA 机构书面允许，他人不得转载用于商业行为；

4) CA 机构对外运营管理策略和规范属于 CA 机构财产。

1) The CA shall have and retain all intellectual property rights such as copyrights and patent application rights for the certificate and all software, materials, data, etc., provided by the CA;

2) CA have ownership and intellectual property rights of CPS, CP, technical support manuals, issued certificates and CRLs formulated and published by the CA;

3) All information published on the official website of the CA belongs to the CA's property. No one else may reprint for commercial activities without the written permission of the CA;

4) CA's external operation management policy and norms belong to CA's property.

.

9.6陈述与担保 Representations and Warranties

9.6.1 电子认证服务机构的陈述与担保 CA Representations and Warranties

CA 机构在提供电子认证服务活动过程中的担保如下:

1) CA 机构遵守《中华人民共和国电子签名法》及相关法律的规定，对签发的数字证书承担相应的法律责任;

2) 验证申请人对列在证书主题字段及主题别名扩展（或，仅针对域名而言，获得了拥有域名所有权或控制权人士的授权）中的域名及 IP 地址拥有所有权或控制权;

3) 验证申请人授权了证书的签发且申请人代表获得了合格授权，以代表申请人申请证书;

4) 验证证书中包含的全部信息的准确性（organizationUnitName 信息除外）;

5) 采取措施以减小证书主题"organizationUnitName"中所含信息存在误导的可能性;

6) 根据本 CPS 第 3.2 节的要求验证申请人身份;

7) 若 CA 机构与订户无关联关系，则 CA 机构与订户是合法有效且可执行的协议双方，该订户协议符合 CA/Browser 论坛发布的 Baseline Requirements

等要求；若 CA 机构与订户为同一实体或有关联，则申请人代表已认可使用条款；

8) CA 机构维护针对所有未过期证书的当前状态信息（有效或已撤销），并据此建立并维护一个全天候的（24 x 7）公开可访问信息库；

9) 根据本 CPS 制定的原因可撤销证书；

10) CA 机构准确描述了证书政策和认证实践声明中的程序；

11) CA 机构签发给订户的证书符合本 CPS 的所有实质性要求；

12) CA 机构将向证书订户通报任何已知的、将在本质上影响订户证书有效性与可靠性的事件；

13) CA 机构拒绝签发证书后，将立即向证书申请人归还所付的全部费用。

The warranties of CAs in the process of providing electronic certification services are as follows:

1) The CA complies with *Electronic Signature Law of the People's Republic of China* and relevant laws, and bears corresponding legal liabilities for the issued digital certificates;

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

3) Verify that the applicant has authorized the issuance of the certificate and that the applicant's representative has obtained a qualified authorization to apply for the certificate on behalf of the applicant;

4) Verify the accuracy of all the information contained in the certificate (except for the organizationUnitName information);

5) Take measures to reduce the possibility of misleading information contained in the certificate subject “organizationUnitName”;

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

7) If the CA and subscriber are not affiliated, the subscriber and CA are parties to a legally valid and enforceable subscriber agreement that satisfies the requirements of

the Baseline Requirements issued by the CA/Browser Forum; if the CA and subscriber are the same entity or are affiliated, the applicant representative has acknowledged the terms of use;

8) The CA maintains a 24 x 7 publicly-accessible repository with current information regarding the status (valid or revoked) of all unexpired certificates;

9) The certificate may be revoked for reasons formulated by this CPS;

10) The CA accurately describes the procedures in the Certificate Policy and Certification Practice Statement;

11) The certificates issued by the CA to the subscriber satisfy all the material requirements of this CPS;

12) The CA will notify the certificate subscriber of any known events that will substantially affect the validity and reliability of the subscriber's certificate;

13) Upon the refusal of the CA to issue the certificate, the CA will immediately return all fees paid to the certificate applicant.

9.6.2 注册机构的陈述与担保 RA Representations and Warranties

作为 CA 机构的注册机构，应遵循 CA 机构的 CPS 与 CP 承担电子认证业务中注册机构的职责，注册机构的电子认证业务操作受行业及 CA 机构的相关管理规定约束。CA 机构的注册机构在参与电子认证服务过程中的具体承诺如下:

1) 注册机构向证书订户提供的注册过程完全符合 CA 机构的 CPS 的所有实质性要求;

2) 如注册机构对订户的证书申请材料未通过审查，注册机构有告知订户的义务;

3) 注册机构在合理期间内完成证书申请处理，在申请人提交资料齐全且合规的情况下，处理证书申请的时间一般为 1-3 个工作日;

4) CA 机构生成证书时，不会由于注册机构的失误而导致证书中的信息与证书申请人的信息不一致;

5) 注册机构将按本 CPS 的规定，及时向 CA 机构提交撤销、更新等申请;

6) 注册机构应通过安全通道将证书订户的信息传送给 CA 机构；

7) 注册机构应妥善保管订户的信息及与认证相关的信息，并适时转交给 CA 机构以存档。注册机构应根据相关协议要求配合 CA 机构进行电子认证业务合规性审计；

8) 注册机构应尽到对订户的安全提示义务。

The RA of the CA shall follow the CPS and CP of the CA to assume the responsibilities of the RA in the electronic certification business. The operation of the electronic certification business of the RA shall be subject to the relevant management regulations of the industry and the CA. The specific commitments of the CA's RA in participating in the electronic certification service process are as follows:

1) The registration process provided by the RA to the certificate subscriber is in full compliance with all the material requirements of the CA's CPS;

2) If subscriber's certificate application materials failed to pass the investigation of the RA, the RA has the obligation to inform the subscriber;

3) The RA completes the certificate application processing within a reasonable period of time. When the applicant submits complete and compliant materials, the time for processing the certificate application is generally 1-3 working days;

4) When the CA generates a certificate, the information in the certificate will not be inconsistent with the information of the certificate applicant due to the mistake of the RA;

5) The RA will submit the application for cancellation and renewal to the CA in time according to the stipulation of this CPS;

6) The RA shall transmit the information of the certificate subscriber to the CA through a secure channel;

7) The RA shall properly keep the subscriber's information and information related to the certification and transfer it to the CA for filing in good time. The RA shall cooperate with the CA to conduct the electronic certification business compliance audit in accordance with the relevant agreements;

8) The RA shall perform its obligation of security warning to the subscriber.

9.6.3 订户的陈述与担保 Subscriber Representations and Warranties

订户自接受 CA 机构签发的证书时起，即视为向 CA 机构、注册机构及信赖

证书的有关当事人作出下述承诺：

1) 订户确认已知悉并接受了本 CPS 及相关规定的全部内容，且同意受本 CPS 条款的约束；

2) 订户应遵循诚实守信原则，在申请数字证书及签发相关的其他方面，都有义务始终向 CA 机构提供准确完整的信息和资料，并在上述信息及资料发生变更时及时通知 CA 机构。如因订户提供的资料不真实、不完整、不准确或变更后未及时通知 CA 机构，由此造成的损失由订户自行承担。如果存在代理人，那么订户和代理人两者负有连带责任。订户有责任就代理人所作的任何不实陈述与遗漏，通知 CA 机构；

3) 订户使用 CA 机构数字证书时，应使用合法途径获取相关软件；

4) 订户应将证书用于合法目的并在有效期内进行数字签名；

5) 订户应通过可靠方式产生密钥对，并有义务采取一切合理措施防止密钥遭受攻击而丢失、泄露和误用；订户应妥善保管 CA 机构签发的数字证书的私钥和密码，不得泄露或交付他人。如因订户原因导致他人知道、盗用、冒用数字证书私钥和密码，由此造成的损失由订户自行承担；

6) 与订户证书所含公钥对应的私钥所进行的每一次签名，都是订户自己的签名，且签名时的证书是有效证书（证书没有过期或被撤销），证书的私钥为订户本身访问和使用；

7) 订户将审查和验证证书内容的准确性，确认其在取得的证书信息无误；

8) 订户在使用证书时，应在证书中列出的可访问的服务器上安装证书，并符合全部使用的法律法规和用户协议约定的使用范围和条件；

9) 不得拒绝任何来自 CA 机构公式过的声明、变更、更新、升级等，包括但不

限于策略、规范的修改和证书服务的增加和删减等；

10) 订户在取得证书后如发现以下情况，应立即向 CA 机构申请撤销：

①有任何实际或可疑的滥用或泄露用户证书中包含的与公钥相对应的私钥，则要求立即撤销证书，并停止使用证书及其相关的私钥；

②证书中的信息不正确或不准确，则要求立即撤销并停止使用证书；

11) 一旦 CA 机构发现了订户证书的不当使用或订户被用于违法甚至犯罪行为，CA 机构有权直接撤销订户证书；

12) 订户保证，一旦证书被 CA 机构撤销后，将不再使用该证书。

From the time the subscriber accepts the certificate issued by the CA, the subscriber is deemed to have made the following commitments to the CA, the RA and the relevant parties trusting the certificate:

1) The subscriber confirms that it has acknowledged and accepted all the content of this CPS and related regulations, and agrees to be bound by the terms of this CPS;

2) Subscribers shall follow the principle of honesty and trustworthiness. They are obliged to always provide accurate and complete information and materials to the CA in applying for digital certificates and other aspects related to issuance, and notify the CA in time when the above information and materials are changed. If the information provided by the subscriber is false, incomplete, inaccurate or not notified to the CA in time after the change, the losses caused by the subscriber shall be borne by the subscriber. If there is an agent, both the subscriber and the agent are jointly and severally liable. The subscriber is responsible for notifying the CA of any misrepresentation or omission made by the agent;

3) When a subscriber uses the CA's digital certificate, the relevant software shall be obtained by legal means;

4) The subscriber shall use the certificate for lawful purposes and digitally sign it within the validity period;

5) The subscriber shall generate the key pair in a reliable manner and shall be obliged to take all reasonable measures to prevent the key from being attacked, lost, disclosed and misused; the subscriber shall properly keep the private key and password of the digital certificate issued by the CA, and shall not disclose or deliver it to others. If others know, misappropriate, or fraudulently use the digital certificate private key and password due to the subscriber's reasons, the losses caused thereby shall be borne by the subscriber;

6) Each signature made by the private key corresponding to the public key contained in the subscriber certificate is the subscriber's own signature, and the certificate used at the time of signing is a valid certificate (the certificate has not expired or is revoked), and the private key of the certificate is used by the subscriber for access and use;

7) The subscriber will review and verify the accuracy of the certificate content and confirm that the certificate information obtained is correct;

8) When using the certificate, the subscriber shall install the certificate on the accessible server listed in the certificate and comply with the scope and conditions of use of all applicable laws and regulations and user agreement;

9) No statements, changes, renewals, upgrades, etc., that have been published by the CA can be rejected, including but not limited to policies, changes to specifications, and additions and deletions of certificate services;

10) If the subscriber finds the following situations after obtaining the certificate, the subscriber shall immediately apply to the CA for revocation:

① promptly request revocation of the certificate and cease using it and its associated private key if there is any actual or suspected misuse or disclosure of the private key corresponding to the public key contained in the user certificate;

② promptly request revocation of the certificate and cease using it if any information in the certificate is incorrect or inaccurate;

11) The CA is entitled to revoke the certificate immediately if the CA discovers that the certificate is misused or the subscriber is being used to enable used it for illegal or even criminal activities;
12) The subscriber warrants to promptly cease all use of the certificate upon it is revoked by the CA.

9.6.4 依赖方的陈述与担保 Relying Party Representations and Warranties

依赖方应作出如下声明和承诺:

1) 熟悉本 CPS 的条款，了解证书的使用目的，遵守本 CPS 的所有规定，同意本 CPS 中关于 CA 机构责任限制的规定;

2) 获取并安装该证书对应的证书链，在信赖证书前，对证书的信任链进行验证;

3) 在信赖证书所证明的信任关系前确认该证书有效，包括：通过查询 CRL 或

OCSP 确认证书是否被撤销；确认证书在规定的范围和期限使用；检查该证书路径中所有出现过的证书的可靠性；确认该证书记载的内容与所要证明的内容一致；检查其他可能影响证书有效性的信息；

4) 不得拒绝任何来自 CA 机构公示过的声明、变更、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等；

5) 依赖方一旦由于疏忽或其他原因违背了合理检查的条款，依赖方应就此给 CA 机构带来的损失进行赔偿，并应承担因此造成的自身或他人损失。

The relying party shall make the following statement and commitment:

1) Familiar with the terms of this CPS, understand the purpose of the certificate use, comply with all the provisions of this CPS, and agree to the stipulation of this CPS regarding the limitation of CA liability;

2) Obtain and install the certificate chain corresponding to the certificate, and verify the certificate's trust chain before trusting the certificate;

3) Confirm that the certificate is valid before relying the trust relationship proved by the certificate, including: confirming whether the certificate is revoked by querying CRL or OCSP; confirming that the certificate is used within the specified scope and period; checking the reliability of all certificates that have appeared in the certificate path; confirming that the content of the certificate are consistent with the content to be certified; checking other information that may affect the validity of the certificate;

4) No statements, changes, renewals, upgrades, etc., that have been published by the CA can be rejected, including but not limited to policies, changes to specifications, and additions and deletions of certificate services;

5) If the relying party violates the terms of the reasonable inspection due to negligence or other reasons, the relying party shall compensate the losses caused to the CA and shall bear the losses caused to itself or others.

9.6.5 其他参与者的陈述与担保 Representations and Warranties of Other Participants

未列于此的其他参与者应遵循本 CPS 的规定。

Other participants not listed here shall follow the stipulation of this CPS.

9.7担保免责 Disclaimers of Warranties

除本 CPS 第 9.6.1 节中的明确承诺外，CA 机构不承担其他任何形式的保证和义务：

1) 不保证证书订户、信赖方及其他参与者的陈述与担保；

2) 不对电子认证活动中使用的任何其他软件做出担保；

3) 不承担超出证书范围使用或用于其他未被 CA 机构允许的用途带来的损失；

4) 不承担超出证书规定目的之外的应用造成的损失；

5) 不承担因非 CA 机构原因导致的设备故障、网络中断导致证书报错、交易中断或其他事物造成的损失；

6) 不承担由于不可抗力因素导致的服务中断并由此造成的客户损失；

7) 明显由于 CA 机构的合作方的越权行为或其他过错行为所引发的违反约定义务而对订户造成的损失，CA 机构不承担责任。

Except for the clear commitments in Section 9.6.1 of this CPS, the CA does not assume any other forms of warranty or obligation:

1) Not warrant the representations and warranties of certificate subscribers, relying parties and other participants;

2) Not warrant any other software used in electronic certification activities;

3) Not bear any losses beyond the scope of the certificate or for other uses not permitted by the CA;

4) Not bear the losses caused by applications beyond the specified purpose of the certificate use;

5) Not bear the losses caused by equipment failures, network interruptions resulting in certificate errors, transaction interruptions or other things that are not because of the CA;

6) Not bear the client losses caused by service interruption due to force majeure factors;

7) The CA is not responsible for the losses caused to the subscribers due to violations of the contractual obligations caused by the CA's partner's ultra vires or other fault actions.

9.8有限责任 Limitations of Liability

如果 CA 机构根据 CPS 或相关法律法规规定，以及司法判定须承担赔偿和/或补偿责任的，CA 机构将承担不超过本 CPS 第 9.9 节规定的有限赔偿责任。

If the CA is required to bear the indemnification and/or compensation liability according to the CPS or relevant laws and regulations and the judicial judgment, the CA institution shall bear the limited liability not exceeding the provisions of Section 9.9 of this CPS.

CA 机构在与订户和依赖方签定的协议中，对于因订户或依赖方的原因造成的损害不具有赔偿义务。

The CA does not have an indemnity obligation in an agreement with a subscriber and a relying party for damages caused by the subscriber or the relying party.

9.9赔偿 Indemnities

9.9.1 CA 机构的赔偿 Indemnification by CAs

如 CA 机构违反了本 CPS 第 9.6.1 节中的陈述与担保，证书订户、依赖方可以申请 CA 机构承担赔偿责任（法定或约定免责除外）。下述情形应由 CA 机构承担有限赔偿责任:

1) CA 机构将证书错误签发给订户以外的第三方，导致订户或依赖方遭受损失;
2) 在订户提交信息或资料完整准确的情况下，CA 机构签发的证书含有错误信息，且导致订户或依赖方由此遭受损失;
3) CA 机构明知订户提交的信息或资料存在虚假谎报的情况，却仍为订户签发证书，由此导致依赖方遭受损失;
4) 由于 CA 机构的原因致使证书私钥的泄露，导致订户或依赖方遭受损失;
5) CA 机构未能及时撤销证书，由此导致依赖方遭受损失。

If the CA violates the representations and warranties in Section 9.6.1 of this CPS, the

certificate subscriber or relying party may apply for the CA to assume liability (except statutory or contractual exemption). The CA shall be liable for limited liability in the following cases:

1) The CA wrongly issued a certificate to a third party other than the subscriber, causing the subscriber or relying party to suffer losses;

2) In the case where the subscriber submits complete and accurate information or materials, the certificate issued by the CA contains error information and causes the subscriber or relying party to suffer losses;

3) In the case where the CA is fully aware that the subscriber has submitted false information or materials and still issues a certificate for the subscriber, causing the relying party to suffer losses;

4) The disclosure of the certificate private key due to the CA causes the subscriber or relying party to suffer losses;

5) The CA failed to revoke the certificate in time, resulting in the loss of the relying party.

9.9.2 订户的赔偿 Indemnification by Subscribers

证书订户在使用或信赖证书时，若有任何行为或疏漏而导致 CA 机构和注册机构产生损失，订户应承担赔偿责任。

When the certificate subscriber uses or trusts the certificate, if there is any action or omission that causes losses to the CA and the RA, the subscriber shall be liable for indemnification.

订户接受证书就表示同意在以下情况下承担赔偿责任。

1) 未向 CA 机构提供真实、完整和准确的信息，而导致 CA 机构或有关各方损失；

2) 未能保护订户的私钥，或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用时，订户必须对这种行为的后果负责；

3) 在知悉证书密钥已经失密或者可能失密时，未及时告知 CA 机构，并终止使用该证书，而导致 CA 机构或有关各方损失；

4) 订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个数字签名后理所当然地相信这些表述，订户必须对这种行为的后果负责；

5) 证书的非法使用，即违反 CA 机构对证书使用的规定，造成了 CA 机构或有关各方的利益受到损失。

Upon acceptance of the certificate, the subscriber agrees to be liable for the following circumstances.

1) Failing to provide true, complete and accurate information to the CA, resulting in losses to the CA or related parties;

2) If the subscriber's private key is not protected, or if the necessary safeguards are not used to prevent the subscriber's private key from being lost, compromised, modified, or used by an unauthorized person, the subscriber must be responsible for the consequences of such conduct;

3) Failing to promptly inform the CA and cease using the certificate when it is aware that the certificate key has been compromised or may be compromised, resulting in losses of the CA or related parties;

4) If the subscriber makes a mistake in describing the information to the relying party, and the relying party takes these descriptions for granted after verifying one or more digital signatures with the certificate, the subscriber must be held liable for the consequences of such conduct;

5) The illegal use of the certificate, that is, the violation of the CA's regulations on the use of the certificate, has caused losses to the interests of the CA or related parties.

9.9.3 依赖方的赔偿 Indemnification by Relying Parties

如因下述情形而导致 CA 机构或订户遭受损失，依赖方应承担赔偿责任：

1) 未履行 CA 机构与依赖方的协议和本 CPS 中规定的义务；

2) 未依照本 CPS 合理审核，导致 CA 机构及其授权的证书服务机构或第三方遭受损失；

3) 在明显不合理的情形下信赖证书，如依赖方明知证书超范围、超期限使用，证书私钥已经或可能被窃取等情形；

4) 依赖方未验证证书的信任链；

5) 依赖方未通过查询 CRL 或 OCSP 验证证书是否被撤销。

If the CA or subscriber suffers losses due to the following circumstances, the relying party shall be liable for indemnification:

1) Failing to perform the agreement between the CA and the relying party and the obligations specified in this CPS;

2) Failing to verify reasonably according to this CPS, resulting in losses suffered by the CA and its authorized certificate service agencies or third parties;

3) Trusting the certificate in an obviously unreasonable situation, such as when the relying party is aware that the use of certificate is out of scope and overdue, and the certificate private key has been or may be stolen;

4) The relying party has not verified the certificate's trust chain;

5) The relying party has not verified whether the certificate has been revoked by querying the CRL or OCSP.

9.10 有效期限与终止 Term and Termination

9.10.1 有效期限 Term

本 CPS 在生效日期零时正式生效，上一版本的 CPS 同时失效。

This CPS comes into effect at 0:00 on the effective date, and the previous version of CPS becomes invalid at the same time.

9.10.2 终止 Termination

CA 机构有权终止本 CPS（含修订版）。本 CPS 在下一版本 CPS 生效之日或在 CA 机构终止电子认证服务时失效。

The CA has the right to terminate this CPS (including amendments). This CPS expires on the date the next version of CPS becomes effective or when the CA terminates the electronic certification service.

9.10.3 效力的终止与保留 Effect of Termination and Survival

本 CPS 终止后，其效力将同时终止，CPS 中的内容将视为无效使用。但对

终止之日前发生的法律事实，CPS 中对各方责任的规定及免除责任仍然有效。CPS 中涉及的审计、保密信息、隐私保护、知识产权等方面继续有效。

After the termination of this CPS, its effect will be terminated at the same time, and the content in the CPS will be considered invalid. However, for the legal facts that occurred before the date of termination, the provisions and the exemption obligations of each party in the CPS are still valid. The audit, confidential information, privacy protection, and intellectual property rights involved in the CPS continue to be valid.

9.11 对参与者的个别通告与沟通 Individual Notices and Communications with Participants

参与者如需进一步了解本 CPS 中提及的条款，可以通过电话联系 CA 机构。

Participants who need to know more about the terms mentioned in this CPS can contact the CA by phone.

本 CPS 终止后，CA 机构将就文档失效的有关事宜通知参与本机构电子认证活动的有关各方。

After the termination of this CPS, the CA will notify the parties involved in the CA's electronic certification activities regarding the invalidation of the documents.

9.12 修订 Amendments

9.12.1 修订程序 Procedure for Amendment

经 CA 机构安全策略管理委员会授权，CPS 编写小组每年至少审查一次本 CPS，确保其符合国家法律法规和主管部门的要求及相关国际标准，确保其符合 CP 要求，符合认证开展的实际业务需要。

Authorized by the CA's Security Policy Administration Committee, the CPS writing team reviews this CPS at least once a year to ensure that: it complies with national laws and regulations and the requirements of the competent authorities and relevant international standards; and it meets the CP requirements and the practice needs of the certification.

本 CPS 的修订与更新，由 CPS 编写小组提出修订报告，经 CA 机构安全策

略管理委员会批准后，由 CPS 编写小组负责组织修订，修订后的 CPS 需经 CA 机构安全策略管理委员会批准后在数字认证公司的网站(http://www.bjca.cn)正式对外发布。

For amending and updating this CPS, the CPS writing team shall submit an amendment report and organize the amendment with the consent of the CA's Security Policy Administration Committee. The amended CPS will be officially published on the website of BJCA (http://www.bjca.cn) after being approved by the CA's Security Policy Administration Committee.

《电子认证业务规则》将进行严格的版本控制。

Certification Practice Statement will be subject to strict version control.

9.12.2 通知机制和期限 Notification Mechanism and Period

修订后的 CPS 经批准后将在 CA 机构的官网 http://www.bjca.cn 上发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，CA 机构将在合理的时间内通知有关各方，合理的时间应保证有关方受到的影响最小。如在修订后发布的 7 个工作日内，订户没有申请对其证书的撤销，将被视为同意该修订。

The amended CPS will be published on the CA's official website http://www.bjca.cn after approval. For amendments that require notification by e-mails, letters, media, etc., the CA will notify the parties within a reasonable time, and the reasonable time shall ensure that the parties concerned are least affected. If within 7 working days after the amendment, the subscriber does not apply for the revocation of its certificate, it will be deemed to agree to the amendment.

9.12.3 必须修改业务规则的情形 Circumstances Under Which CPS Must Be Changed

1) 本 CPS 中相关内容与管辖的法律法规或部门规章不一致，CA 机构将据此修改本 CPS 中的相关内容；

2) 国家监管部门对本 CPS 由明确的更改或调整要求；

3) 本 CPS 描述的规则、流程和相关技术已经不能满足 CA 机构电子认证业务的要求；

4) 本 CPS 中相关内容与 CA/Browser 论坛最新发布的相关规范、WebTrust 对 CA 的规则不一致，CA 机构将据此修改本 CPS 中的相关内容。

1) The relevant content in this CPS is inconsistent with the laws, regulations or departmental rules of the jurisdiction, and the CA will modify the relevant content in this CPS accordingly;

2) The national regulatory authorities have a clear request of change or adjustment for this CPS;

3) The rules, procedures and related technologies described in this CPS no longer meet the requirements of the CA's electronic certification business;

4) The relevant content in this CPS is inconsistent with the latest specifications of the CA/Browser Forum and the rules of WebTrust for CA. The CA will modify the relevant content in this CPS accordingly.

9.13 争议处理 Dispute Resolution Provisions

CA 机构、证书订户、依赖方等实体在电子认证活动中产生争议时，应在争议产生之时起 3 个月内向 CA 机构提出争议处理请求并通知有关各方，争议解决的方式可按如下步骤：

1) 根据本 CPS 及相关法律法规的规定，明确责任方；

2) 由 CA 机构相关部门负责与申请人协调；

3) 若 CA 机构协调失败，再由有关法律部门进行裁决；

4) 任何与 CA 机构或注册机构就本 CPS 所涉及的任何争议，争议双方仅可以将争议提交北京仲裁委员会仲裁。

Disputes arising from electronic certification activities by entities such as CAs, certificate subscribers and relying parties shall file a dispute resolution request with the CA within 3 months from the time of the dispute and notify the relevant parties. The dispute resolution can be implemented in the following steps:

1) According to the provisions of this CPS and relevant laws and regulations, the

responsible party is clearly defined;

2) The relevant departments of the CA are responsible for coordinating with the applicant;

3) If the coordination of the CA fails, the relevant legal department will make a ruling;

4) For any dispute with the CA or the RA regarding this CPS, the parties to the dispute may only submit the dispute to the Beijing Arbitration Commission for arbitration.

9.14 管辖法律 Governing Law

CA 机构的 CPS 受国家已颁布的《中华人民共和国民法典》、《中华人民共和国电子签名法》和《电子认证服务管理办法》及相关法律法规规定。如本 CPS 中某项条款与上述法律法规条款或其可执行性发生抵触，CA 机构将对此条款进行修订，使之符合相关法律法规规定。

The CPS of CA is subject to *Civil Code of the People's Republic of China*, *Electronic Signature Law of the People's Republic of China* and *Measures for the Administration of Electronic Certification Service* and relevant laws and regulations. If a clause in this CPS conflicts with the provisions of the above-mentioned laws and regulations or its enforceability, the CA will amend the clause to comply with relevant laws and regulations.

9.15 与适用法律的符合性 Compliance with Applicable Law

无论 CA 机构的证书订户、依赖方等实体在何地居住以及在何处使用 CA 机构的证书，本 CPS 的执行、解释和程序有效性均适用中华人民共和国法律规定。任何与 CA 机构或授权注册机构就本 CPS 所涉及的任何争议，均应适应中华人民共和国法律。

The implementation, interpretation and procedural validity of this CPS shall be governed by the laws of the People's Republic of China, regardless of where the CA's certificate subscribers, relying parties and other entities reside and where they use the CA's certificate. Any dispute with the CA or the authorized RA regarding this CPS shall be resolved in accordance with the laws of the People's Republic of China.

9.16 一般条款 Miscellaneous Provisions

9.16.1 完整协议 Entire Agreement

CA 机构的 CPS 完整的文档结构包括：标题、目录、主体内容 3 部分。关于对目录和主体内容修改后的替代内容，将完全替代所有先前部分。本 CPS 将替代所有以前的或同时期的、相同主题的书面或口头解释。本完整协议将放置在 CA 机构的官方网站中以供查询和浏览。

The complete document structure of CA's CPS includes 3 parts: title, contents and body content. The modified alternatives to the contents and body content will completely replace all previous Sections. This CPS will replace all previous or contemporaneous written or oral interpretations of the same subject. This complete agreement will be published on the official website of the CA for query and browsing.

9.16.2 转让 Assignment

CA 机构声明，根据本 CPS 中详述的认证实体各方的权利和义务，各方当事人可按照法律法规的相关规定进行权利与义务的转让。此转让行为发生时不影响转让方对另一方的任何债务及责任的更新。

The CA declares that, according to the rights and obligations of the parties to the certification entity detailed in this CPS, the parties may assign the rights and obligations in accordance with the relevant provisions of laws and regulations. This assignment does not affect the assignor’s renewal of any debts and liabilities of the other party.

9.16.3 分割性 Severability

本 CPS 的任何条款或应用由于与 CA 机构所在管辖权的法律法规发生冲突而被判定为无效或不具有执行力时，CA 机构可以在最低必要的限度下修订该条款，使其继续有效，其余部分不受影响，CA 机构将在此章节披露修订的内容。

When any clause or application of this CPS is determined to be invalid or non-executive due to conflicts with the laws and regulations of the jurisdiction in

which the CA is located, the CA may amend the clause to the extent necessary to continue to be effective, with the rest unaffected, the CA will disclose the amended content in this Section.

在根据修订后要求签发证书之前，CA 机构将发送邮件至 questions@cabforum.org，通知 CA/Browser 论坛 CPS 中已修订的信息，并确认已将其发布到公共邮件列表和公共档案列表 https://cabforum.org/pipermail/public/。

Before issuing a certificate based on the amended request, the CA will send an email to questions@caforum.org, notify the CA/Browser Forum CPS of the amended information, and confirm that it has been posted to the public mailing list and public file list https:// /cabforum.org/pipermail/public/.

若法律不再适用，或 CA/Browser 论坛的要求被修改，使 CA 机构同时符合 CA/Browser 论坛的 Baseline Requirements 及法律要求，则本章节中任何对 CA 机构业务操作的调整将不再适用。上述对业务操作进行的相关调整，对 CA 机构的 CPS 的修订，及向 CA/Browser 论坛的通知将在 90 天内完成。

If the law no longer applies, or the requirements of the CA/Browser Forum are modified to make the CA conform to both the Baseline Requirements and legal requirements of the CA/Browser Forum, any adjustments to the business operations of the CA in this Section will no longer apply. The above-mentioned related adjustments to the business operations, the amendment of the CA's CPS, and the notification to the CA/Browser Forum will be completed within 90 days.

9.16.4 强制执行 Enforcement

CA 机构声明，若订户证书、依赖方等实体未执行 CA 机构的 CPS 中某项规定，不被认为该实体将来不执行该项或其他规定。

The CA declares that if the entity such as the subscriber certificate or relying party fails to implement a provision in the CPS of the CA, it is not considered that the entity will not implement the or other provisions in the future.

9.16.5 不可抗力 Force Majeure

CA 机构不对因战争、恐怖活动、自然灾害、传染性疾病、罢工、互联网或

其他基础设施无法使用等不可抗力的事件所造成本 CPS 规定担保责任的违反、延误或无法履行负责。

The CA shall not be liable for violations, delays or failure to perform the warranty obligations of this CPS due to force majeure events such as wars, terrorist activities, natural disasters, infectious diseases, strikes, breakdown of Internet or other infrastructure.

9.17 其他条款 Other Provisions

CA 机构对本 CPS 具有最终解释权。

The CA reserves the right to the final interpretation of this CPS.