数安时代科技股份有限公司

证书策略

版本：3.4

发布日期：2025 年 11 月 5 日

Global Digital Cybersecurity Authority CO., LTD.

Certificate Policy (CP)

Version: 3.4

Release Date: November 5, 2025

目录

Contents

1. 引言 Introduction

1.1. 概述 Overview

1.1.1. 公司简介 Company Profile

数安时代科技股份有限公司（Global Digital Cybersecurity Authority Co., Ltd.），简称 GDCA 或“数安时代”）原为“广东数字证书认证中心有限公司”，成立于 2003 年 3 月 6 日。2005 年 9 月，GDCA 依法通过了国家密码管理局和原国家信息产业部的资格审查，成为全国首批八家获得《电子认证服务许可证》（许可证号：ECP44010215007）的电子认证服务机构之一；2008 年 12 月，获得国家密码管理局颁发的《商用密码产品销售许可证》；2011 年 4 月，通过了国家密码管理局电子政务电子认证服务能力评估，获得《电子政务电子认证服务机构》（编号：A021）资格。2013 年，对电子认证服务系统进行 SM2 算法升级，并通过了国家密码管理局组织的安全性审查。2015 年初，GDCA 通过了 WebTrust 国际安全审计认证，具备了国际标准化的运营管理和服务水平，可以提供全球化的电子认证服务。为适应业务发展需要，2016 年 5 月，“广东数字证书认证中心有限公司”更名为“数安时代科技股份有限公司”。2017 年 8 月 11 日，GDCA 在新三板挂牌交易，股票简称：数安时代，股票代码：871932。

Global Digital Cybersecurity Authority CO., LTD. (abbreviated as GDCA, or “数安时代”) with the former name of Guangdong Digital Certificate Authority CO., LTD was founded on March 6, 2003. In September 2005, GDCA passed the security review by the State Cryptography Administration Office of Security Commercial Code Administration (abbreviated as OSCCA) and the former Ministry of Information Industry by law, as one of the first eight electronic authentication authorities with "Electronic Authentication Service License" (license number: ECP44010215007) in China. In December 2008, GDCA obtained the "Commercial Cryptography Products Sales License" issued by OSCCA. GDCA passed through the assessment of E-government and Electronic Authentication Service Ability by OSCCA with the qualification certificate of "E-government and Electronic Authentication Service Authority" (number: A021) in April 2011. In 2013, GDCA upgraded electronic authentication service system for SM2 algorithm and passed through the security review by OSCCA. In 2015, GDCA passed the assurance review for Certification Authority by WebTrust with the international level of operation management and service to provide digital certification service globally. For business development, GDCA changed its name from "Guangdong Digital Certificate Authority CO., LTD." to "Global Digital Cybersecurity Authority CO., LTD." in May, 2016. On 11 August 2017, GDCA was admitted to the National Equities Exchange and Quotations (NEEQ) of China, with a stock abbreviation of “数安时代” and stock code “871932”.

GDCA 更名后，原“广东数字证书认证中心有限公司”的资产、债务、权益和经营业务

全部由“数安时代科技股份有限公司”承继。在更名前与 GDCA 以“广东数字证书认证中心有限公司”名义签订的合同、协议项下应由“广东数字证书认证中心有限公司”享有的权利和承担的义务均由“数安时代科技股份有限公司”承继。

Since then, all assets, debt, rights and business of "Guangdong Digital Certificate Authority CO., LTD." were inherited by GDCA. Meanwhile, and all the rights and obligations of the contracts and agreements signed by "Guangdong Digital Certificate Authority CO., LTD." were inherited by GDCA.

数安时代秉持“权威、公信、专业、创新”的企业价值观，履行“信任联接天下”的企业使命，致力于成为“一流的网络信任服务商”。

GDCA upholds the corporate values of “Authority, Credibility, Professionalism, and Innovation”, fulfils the corporate mission of “Trust Connects Parties from all over the World”, and is committed to becoming a “first-class online trust service provider”.

1.1.2. 证书策略 Certificate Policy (CP)

本文件描述 GDCA 的证书策略（CP），是 GDCA 数字证书服务的策略声明，适用于所有由 GDCA 签发和管理的数字证书及相关参与主体。为批准、签发、管理、使用、更新、撤销证书和相关的可信服务制定业务、法律和技术上的要求和规范。这些要求和规范保护 GDCA 数字证书服务的安全性和完整性，包含一整套在 GDCA 范围内一致适用的单一规则集，因此在整个 GDCA 架构内能够提供同样的信任担保。本 CP 并不是 GDCA 和各参与方之间的法律性协议，GDCA 和各参与方之间的权利义务依靠他们之间签署的各类协议构成。

This document describes the Certificate Policy (CP) of GDCA and explains the policy statement for GDCA digital certificate service. It applies to all digital certificates issued and managed by GDCA and their related participants. The CP sets forth business, legal and technical requirements and specifications for certificate approval, issuance, management, usage, renewal, revocation and related trusted services. These requirements and specifications protects the security and integrity of GDCA digital certificate services and includes a comprehensive set of consistently applicable single rule sets in the GDCA scope. Therefore it provides the same extent of trust guarantee throughout the GDCA architecture. The CP is not a legal agreement between GDCA and all participants; contractual rights and obligations between GDCA and participants are established by other means of agreements with such participants.

本 CP 满足《互联网 X.509 公开密钥基础设施证书策略和证书业务框架》（Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework），即由互联网标准组织“互联网工程工作组”（Internet Engineering Task Force）制定的 RFC3647 标准的结构和内容要求，同时也满足《GB 26855-2011-T 信息安全技术公钥基础设施证书策略与认证业务声明框架》的结构和内容要求，并根据中国的法律法规和 GDCA 的运营要求进行适当的改变。

The CP complies with the structure and content requirements of both Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, also called RFC3647 defined by The Internet Engineering Task Force, and GB 26855-2011-T Information Security Technology Public Key Infrastructure Certificate Policies and Certification Practice Statement Framework. It would also make appropriate changes in accordance with Chinese laws and regulations together with operational requirements of GDCA.

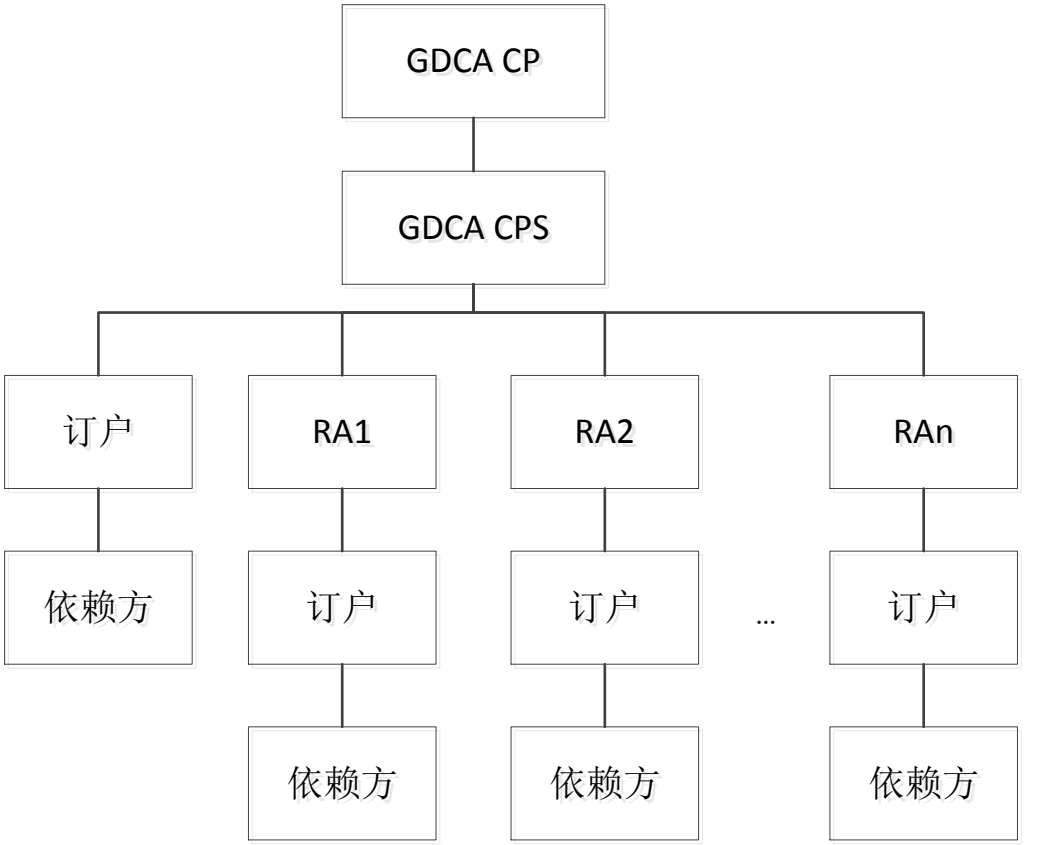
GDCA 作为一个证书服务机构（CA），在本 CP 的约束下生成根证书和 CA 证书，签发订户证书。基于不同的类型和应用范围，作为证书持有人的订户可以使用证书进行网络站点安全保护、代码签名、邮件签名、文档签名、身份认证等不同的应用。依赖方依照本 CP 中关于依赖方的义务要求，决定是否信任一张证书。GDCA 的电子认证业务规则（CPS）接受本 CP 的约束，详细阐述了 GDCA 作为电子认证服务机构提供的证书、如何提供证书以及相应的管理、操作和保障措施。所有 GDCA 证书的订户及依赖方必须参照本 CP 及相关 CPS 的规定，决定对证书的使用和信任。

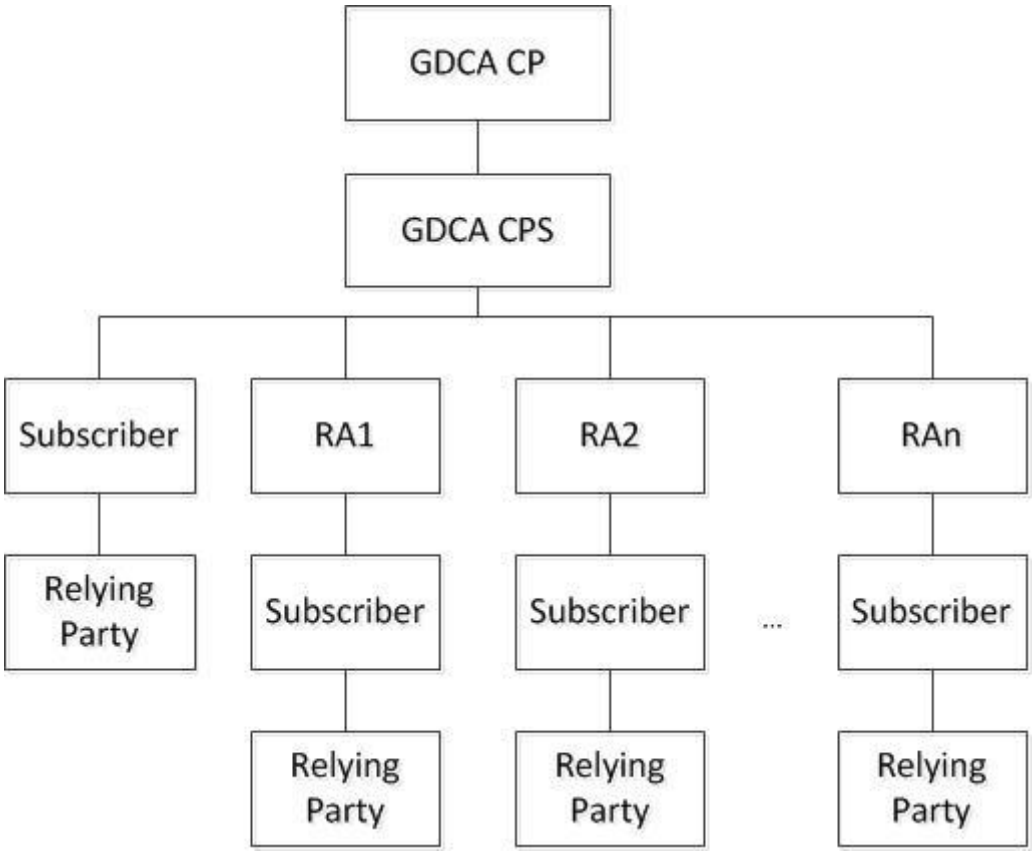
As a Certification Authority (CA), GDCA generates root and intermediate certificates, and issues certificates to subscribers under CP restrictions. Based on different types and application scope, digital certificates may be used by subscribers to process SSL, code signing, e-mail signing, document signing, identity authentication, and other different applications. Relying party could decide whether to trust a certificate in accordance with the requirements of the relying party's obligations in this CP. GDCA Certification Practice Statement (CPS) accept the discipline of CP, elaborates the definition of GDCA digital certificates and the methods to provide these certificates as well as the corresponding managerial, operational and security measures. All certificate subscribers and relying parties under GDCA must refer to the provisions of the CP and its relevant CPS to determine the usage and reliability of the certificates.

1.1.3. GDCA 架构 GDCA Architecture

本 CP 是 GDCA 最高的策略，GDCA 的证书服务机构（CA）按照 CP 制定 CPS，RA 按照本 CP 及相关 CPS 进行证书服务申请鉴别，订户、依赖方及其他相关实体按照本 CP 及相关 CPS 决定对证书的使用、信任并履行相关的义务。GDCA 包含了根 CA、中级 CA，各相关注册机构、分中心、业务受理点，这些实体都是 GDCA 认证体系内不同层次的服务主体。

The CP is the highest strategy throughout the GDCA architecture. Certification authority (CA) under GDCA formulates CPS in accordance with CP. Registration Authority (RA) authenticates certification requests according to this CP and its related CPS. Subscribers, relying parties along with other correlative entities determine their rights for using and trusting the certificates as well as perform corresponding obligations on the basis of the CP and its related CPS. GDCA has established services entities at different levels, including root CA, subordinate CA, related RA, registration authority terminals and business acceptance points.


GDCA CP
GDCA CPS
订户
RA1
RA2
RAn
依赖方
订户
订户
...
订户
依赖方
依赖方
依赖方

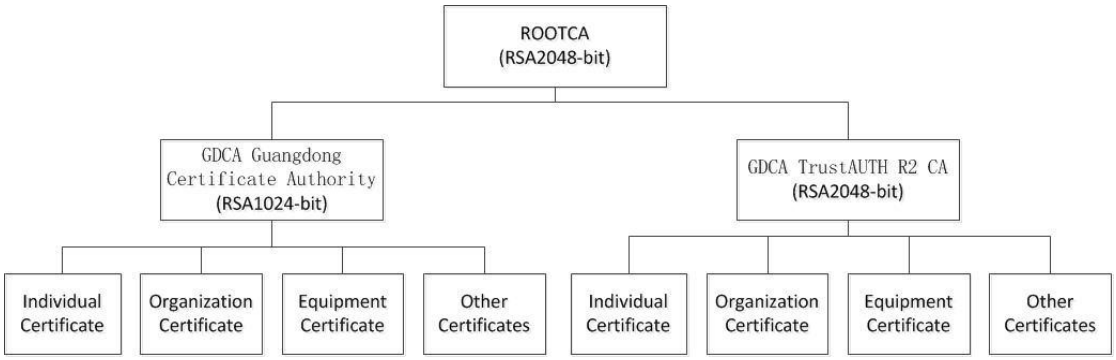

GDCA CP
GDCA CPS
Subscriber
RA1
RA2
RAn
Relying Party
Subscriber
Subscriber
...
Subscriber
Relying Party
Relying Party
Relying Party

1.1.4. GDCA 证书层次架构 Hierarchical Architecture of GDCA Certificates

GDCA 目前有 7 个根证书，分别为 ROOTCA 证书（RSA）、GDCA ROOT CA 证书、ROOTCA 证书（SM2）、GDCA ROOT CA1 证书、GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 证书。每个根 CA 下设中级 CA，以签发用户证书。GDCA 不签发外部中级 CA 证书。

Currently, GDCA has 7 root certificates, including ROOTCA certificate(RSA), GDCA ROOT CA certificate, ROOTCA certificate(SM2) , GDCA ROOT CA1 certificate, GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA certificate and GDCA TrustAUTH E5 ROOT certificate. Each Root CA has Subordinate CAs to issue subscriber certificates. GDCA does not issue external Subordinate CAs.

1) ROOTCA（RSA）



ROOTCA(RSA)证书是国家密码管理局的根证书，密码算法为 RSA，根密钥长度为 2048-bit，下设两个中级 CA 证书，其中：（1）GDCA Guangdong Certificate Authority 证书，密钥长度为 1024-bit，签发密钥长度为 RSA 1024-bit 的个人类证书、机构类证书、设备类证书和其他类证书；（2）GDCA TrustAUTH R2 CA 证书，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 和 RSA 1024-bit 的个人类证书、机构类证书、设备类证书和其他类证书。

ROOTCA (RSA) certificate is a root certificate of OSCCA using RSA algorithm with 2048-bit root key length. There are two subordinate CAs under this ROOT CA, including: (1) GDCA Guangdong Certificate Authority certificate with 1024-bit key length is used for issuing RSA 1024-bit individual certificates, organization certificates, equipment certificates and other certificates. (2) GDCA TrustAUTH R2 CA certificate with 2048-bit key length is used for issuing RSA 2048-bit and RSA 1024-bit individual certificates, organization certificates, equipment certificates and other certificates.

RSA ROOTCA(RSA)证书将于 2025 年 8 月 23 日到期。

ROOTCA certificate (RSA) will expire on August 23, 2025.

GDCA Guangdong Certificate Authority 证书于 2015 年 7 月 19 日到期，2015 年 1 月 1 日起，GDCA 不再使用该 CA 证书签发订户证书。GDCA TrustAUTH R2 CA 证书于 2018 年 12 月 15 日到期，2017 年 12 月 15 日起，GDCA 不再使用该 CA 证书签发订户证书。

GDCA Guangdong Certificate Authority certificate expired on July 19, 2015. From January 1, 2015, GDCA no longer used it to issue subscriber certificates. GDCA TrustAUTH R2 CA certificate expired on December 15, 2018. From December 15, 2017, GDCA no longer used it to issue subscriber certificates.

2) GDCA ROOT CA（1024-bit）

GDCA ROOT CA 证书的根密钥长度为 1024-bit，下设 GDCA Guangdong Certificate Authority 证书，密钥长度为 1024-bit，签发密钥长度为 RSA 1024-bit 的个人类证书、机构类证书、设备类证书和其他类证书。

The length of GDCA ROOT CA certificate root key is 1024-bit. There is a GDCA Guangdong Certificate Authority certificate under this ROOT CA, used for issuing RSA 1024-bit individual certificates, organization certificates, equipment certificates and other certificates.

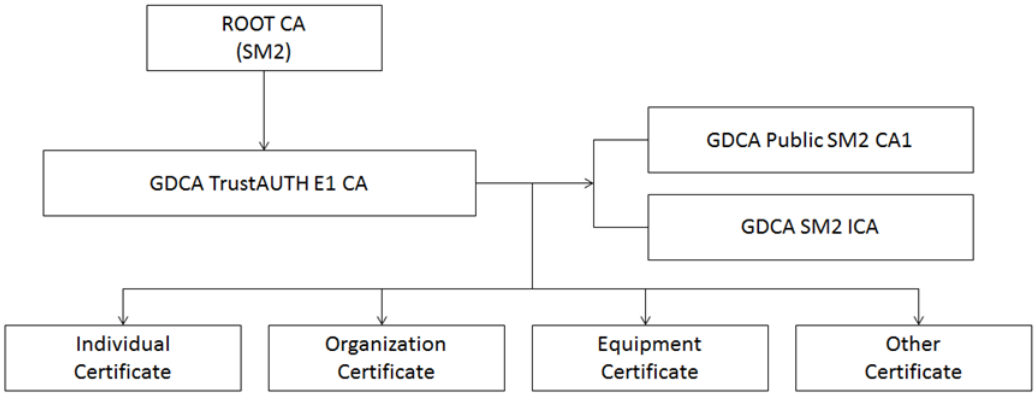
GDCA ROOT CA 证书于 2024 年 12 月 11 日到期。

GDCA ROOT CA certificate expired on December 11, 2024.

GDCA Guangdong Certificate Authority 证书于 2024 年 1 月 12 日到期，2016 年 1 月 1 日起，不再使用该 CA 证书签发订户证书。

GDCA Guangdong Certificate Authority certificate expired on January 12, 2024. From January 1, 2016, GDCA no longer uses it to issue subscriber certificates.

3) ROOTCA（SM2）



ROOTCA 证书（SM2）是国家密码管理局的根证书，密码算法为 SM2，根密钥长度为 256-bit，下设 Guangdong Certificate Authority（GDCA TrustAUTH E1 CA）证书，密钥长度为 256-bit，签发采用国密算法 SM2 的个人类证书、机构类证书、设备类证书和其他类证书，Guangdong Certificate Authority（GDCA TrustAUTH E1 CA）下设 GDCA SM2 ICA 证书及 GDCA Public SM2 CA1 证书，签发采用国密算法 SM2 的个人类证书、机构类证书、设备类证书和其他类证书。

ROOTCA (SM2) certificate is a root certificate of OSCCA using SM2 algorithm with root key length of 256-bit. There is a Guangdong Certificate Authority (GDCA TrustAUTH E1 CA SM2) certificate with key length of 256-bit under this root CA, used for issuing individual certificates, organization certificates, equipment certificates and other certificates with SM2 algorithm. Guangdong Certificate Authority (GDCA TrustAUTH E1 CA) issued GDCA SM2 ICA and GDCA Public SM2 CA1, which are used for issuing individual certificates, organization certificates, equipment certificates and other certificates with SM2 algorithm.

ROOTCA 证书（SM2）将于 2042 年 7 月 7 日到期。

ROOTCA (SM2) will expire on July 7, 2042.

Guangdong Certificate Authority（GDCA TrustAUTH E1 CA）证书将在 2034 年 6 月 21 日到期，2030 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

Guangdong Certificate Authority (GDCA TrustAUTH E1 CA) certificate will expire on June 21, 2034. From January 1, 2030, GDCA will no longer use it to issue subscriber certificates.

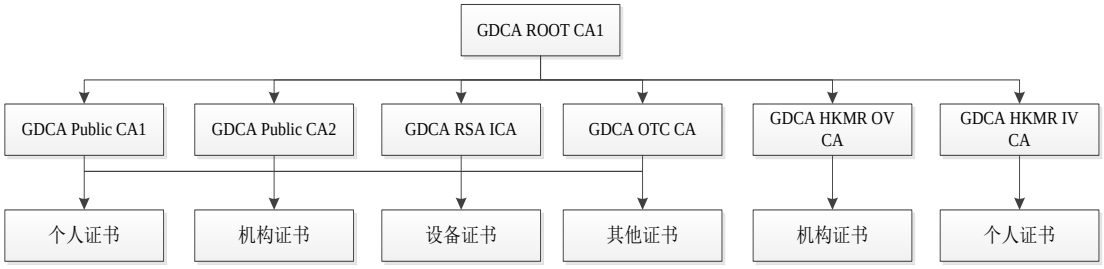
GDCA SM2 ICA 证书将在2033年12月31日到期，2030 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA SM2 ICA certificate will expire on December 31, 2033. From January 1, 2030, GDCA will no longer use it to issue subscriber certificates.

GDCA Public SM2 CA1 证书将在2033年12月31日到期，2030 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA Public SM2 CA1 certificate will expire on December 31, 2033. From January 1, 2030, GDCA will no longer use it to issue subscriber certificates.

4) GDCA ROOT CA1



GDCA ROOT CA1 证书的根密钥长度为 4096-bit，下设 6 个中级 CA 证书，其中：（1）GDCA Public CA1，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的个人类证书、机构类证书、设备类证书和其他类证书；（2）GDCA Public CA2，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的个人类证书、机构类证书、设备类证书和其他类证书；（3）GDCA HKMR OV CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的粤港互认机构证书；（4）GDCA HKMR IV CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的粤港互认个人证书；（5）GDCA RSA ICA 密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的个人类证书、机构类证书、设备类证书和其他类证书；（6）GDCA OTC CA 密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的个人类证书和机构类证书、设备类证书和其他类证书。

GDCA ROOT CA1 证书将于 2040 年 12 月 31 日到期。

GDCA Public CA1 证书将在 2038 年 12 月 31 日到期，2035 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA Public CA2 证书将在 2038 年 12 月 31 日到期，2035 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA HKMR OV CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA HKMR IV CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA RSA ICA 证书将在2030年12月31日到期，2028 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA OTC CA 证书将在2030年12月31日到期，2028 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

粤港互认证书策略遵循最新版的《粤港电子签名证书互认证书策略》，本 CP 不再描述。

The length of GDCA ROOT CA1 certificate root key is 4096-bit. There are six subordinate CAs under this root CA, including: (1) GDCA Public CA1 with key length of 2048 bit, used for issuing RSA 2048-bit individual certificates, organization certificates, equipment certificates and other certificates; (2) GDCA Public CA2 with key length of 2048 bit, used for issuing RSA 2048-bit individual certificates, organization certificates, equipment certificates and other certificates; (3) GDCA HKMR OV CA with key length of 2048-bit, used for issuing RSA 2048-bit organization certificates for Guangdong – Hong Kong mutual recognition purpose; (4) GDCA HKMR IV CA with key length of 2048-bit, used for issuing RSA 2048-bit individual certificates for Guangdong – Hong Kong mutual recognition purpose; (5) GDCA RSA ICA with key length of 2048-bit, used for issuing RSA 2048-bit individual certificates, organization certificates, equipment certificates and other certificates. (6) GDCA OTC CA with key length of 2048-bit, used for issuing RSA 2048-bit individual certificates, organization certificates, equipment certificates and other certificates.

GDCA ROOT CA1 will expire on December 31, 2040.

GDCA Public CA1 will expire on December 31, 2038, and from January 1, 2035, GDCA will no longer use it to issue subscriber certificates.

GDCA Public CA2 will expire on December 31, 2038, and from January 1, 2035, GDCA will no longer use it to issue subscriber certificates.

GDCA HKMR OV CA will expire on December 31, 2030, and from January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

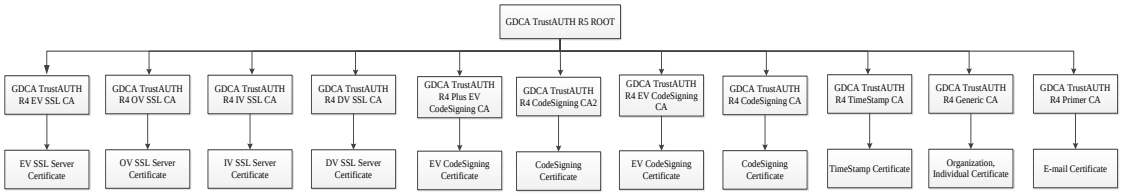
GDCA HKMR IV CA will expire on December 31, 2030, and from January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

GDCA RSA ICA will expire on December 31, 2030 and from January 1, 2028, GDCA will no longer use it to issue subscriber certificates.

GDCA OTC CA will expire on December 31, 2030 and from January 1, 2028, GDCA will no longer use it to issue subscriber certificates.

The certificate policy for the Hong Kong and Guangdong Mutual Recognition conforms to the latest version of the *Guangdong the Certificate Policy for Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong.*

5) GDCA TrustAUTH R5 ROOT



GDCA TrustAUTH R5 ROOT 证书的根密钥长度为 4096-bit，下设 11 个中级 CA 证书，其中：（1）GDCA TrustAUTH R4 EV SSL CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 EV SSL 服务器类证书；（2）GDCA TrustAUTH R4 OV SSL CA 证书，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 OV SSL 服务器类证书；（3）GDCA TrustAUTH R4 IV SSL CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 IV SSL 服务器类证书；（4）GDCA TrustAUTH R4 DV SSL CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 DV SSL 服务器类证书；（5）GDCA TrustAUTH R4 Plus EV CodeSigning CA 证书，密钥长度为 4096-bit，签发密钥长度为 RSA 3072-bit 的 EV 代码签名类证书；（6）GDCA TrustAUTH R4 CodeSigning CA2 证书，密钥长度为 4096-bit，签发密钥长度为 RSA 3072-bit 的代码签名类证书；（7）GDCA TrustAUTH R4 EV CodeSigning CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 EV 代码签名类证书；（8）GDCA TrustAUTH R4 CodeSigning CA 证书，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的代码签名类证书；（9）GDCA TrustAUTH R4 TimeStamp CA 证书，密钥长度为 4096-bit，签发密钥长度为 RSA 3072-bit 的时间戳证书；（10）GDCA

TrustAUTH R4 Generic CA 证书，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的机构、个人类证书；（11）GDCA TrustAUTH R4 Primer CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 S/MIME 安全邮件证书。

The length of GDCA TrustAUTH R5 ROOT certificate root key is 4096-bit. There are eleven subordinate CAs under this root CA, including: (1) GDCA TrustAUTH R4 EV SSL CA with key length of RSA 2048-bit is used for issuing RSA 2048-bit EV SSL Server Certificates. (2) GDCA TrustAUTH R4 OV SSL CA with key length of 2048-bit is used for issuing RSA 2048-bit OV SSL Server Certificates. (3) GDCA TrustAUTH R4 IV SSL CA with key length of 2048-bit is used for issuing RSA 2048-bit IV SSL Server Certificates. (4) GDCA TrustAUTH R4 DV SSL CA with key length of 2048-bit is used for issuing RSA 2048-bit DV SSL Server Certificates. (5) GDCA TrustAUTH R4 Plus EV CodeSigning CA with key length of 4096-bit is used for issuing RSA 3072-bit EV CodeSigning Certificates. (6) GDCA TrustAUTH R4 CodeSigning CA2 with key length of 4096-bit is used for issuing RSA 3072-bit CodeSigning Certificates. (7) GDCA TrustAUTH R4 EV CodeSigning CA with key length of 2048-bit is used for issuing RSA 2048-bit EV CodeSigning Certificates. (8) GDCA TrustAUTH R4 CodeSigning CA with key length of 2048-bit is used for issuing RSA 2048-bit CodeSigning Certificates. (9) GDCA TrustAUTH R4 TimeStamp CA with key length of 4096-bit is used for issuing RSA 3072-bit Timestamp Certificates. (10) GDCA TrustAUTH R4 Generic CA with key length of 2048-bit is used for issuing RSA 2048-bit Organization, Individual Certificates. (11) GDCA TrustAUTH R4 Primer CA with key length of 2048-bit is used for issuing RSA 2048-bit S/MIME Certificates.

GDCA TrustAUTH R5 ROOT 证书将于 2040 年 12 月 31 日到期。

GDCA TrustAUTH R5 ROOT certificate will expire on December 31, 2040.

GDCA TrustAUTH R4 EV SSL CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH R4 EV SSL CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

GDCA TrustAUTH R4 OV SSL CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH R4 OV SSL CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

GDCA TrustAUTH R4 IV SSL CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH R4 IV SSL CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

GDCA TrustAUTH R4 DV SSL CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH R4 DV SSL CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

GDCA TrustAUTH R4 Plus EV CodeSigning CA 证书将在 2035 年 12 月 31 日到期，2032 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH R4 Plus EV CodeSigning CA certificate will expire on December 31, 2035. From January 1, 2032, GDCA will no longer use it to issue subscriber certificates.

GDCA TrustAUTH R4 CodeSigning CA2 证书将在 2040 年 2 月 10 日到期，2037 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH R4 CodeSigning CA2 certificate will expire on February 10, 2040. From January 1, 2037, GDCA will no longer use it to issue subscriber certificates.

GDCA TrustAUTH R4 EV CodeSigning CA 证书将在 2030 年 12 月 31 日到期，2021 年 6 月 1 日起，已不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH R4 EV CodeSigning CA certificate will expire on December 31, 2030. As of June 1, 2021, GDCA has stopped the issucane of subscriber certificates with this CA certificate.

GDCA TrustAUTH R4 CodeSigning CA 证书将在 2030 年 12 月 31 日到期，2021 年 6 月 1 日起，已不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH R4 CodeSigning CA certificate will expire on December 31, 2030. As of June 1, 2021, GDCA has stopped the issucane of subscriber certificates with this CA certificate.

GDCA TrustAUTH R4 TimeStamp CA 证书将在 2035 年 12 月 31 日到期，2032 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH R4 TimeStamp CA certificate will expire on December 31, 2035. From January 1, 2032, GDCA will no longer use it to issue subscriber certificates.

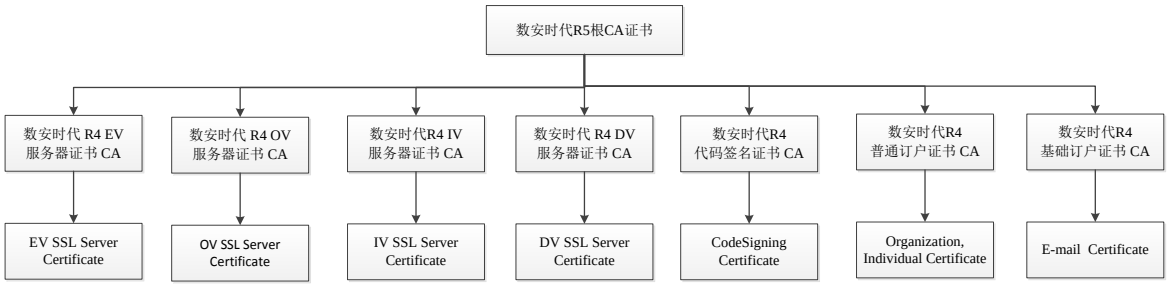
GDCA TrustAUTH R4 Generic CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH R4 Generic CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

GDCA TrustAUTH R4 Primer CA 证书将在 2030 年 12 月 31 日到期，2024 年 4 月 4 日起，已不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH R4 Primer CA certificate will expire on December 31, 2030. GDCA no longer used it to issue subscriber certificates as of April 4, 2024.

6) 数安时代 R5 根 CA



数安时代 R5 根 CA 证书的根密钥长度为 4096-bit，下设 7 个中级 CA 证书，其中：（1）数安时代 R4 EV 服务器证书 CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 EV SSL 服务器类证书；（2）数安时代 R4 OV 服务器证书 CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 OV SSL 服务器类证书；（3）数安时代 R4 IV 服务器证书 CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 IV SSL 服务器类证书；（4）数安时代 R4 DV 服务器证书 CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 DV SSL 服务器类证书；（5）数安时代 R4 代码签名证书 CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的代码签名类证书；（6）数安时代 R4 普通订户证书 CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的机构、个人类证书；（7）数安时代 R4 基础订户证书 CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的 S/MIME 安全邮件证书。

The length of 数安时代 R5 根 CA certificate root key is 4096-bit. There are seven subordinate CAs under this root CA, including: (1) 数安时代 R4 EV 服务器证书 CA with key length of 2048-bit is used for issuing RSA 2048-bit EV SSL Server Certificates. (2) 数安时代 R4 OV 服务器证书 CA with key length of 2048-bit is used for issuing RSA 2048-bit OV SSL Server Certificates. (3) 数安时代 R4 IV 服务器证书 CA with key length of 2048-bit is used for RSA 2048-bit IV SSL Server Certificates. (4) 数安时代 R4 DV 服务器证书 CA with key length of 2048-bit is used for issuing RSA 2048-bit DV SSL Server Certificates. (5) 数安时代 R4 代码签名证书 CA with key length of 2048-bit is used for issuing RSA 2048-bit CodeSigning Certificates. (6) 数安时代 R4 普通订户证书 CA with key length of 2048-bit is used for issuing RSA 2048-bit Organization, Individual Certificates. (7) 数安时代 R4 基础订户证书 CA with key length of 2048-bit is used for issuing RSA 2048-bit S/MIME Certificates.

数安时代 R5 根 CA 证书将于 2040 年 12 月 31 日到期。

数安时代 R5 根 CA certificate will expire on December 31, 2040.

数安时代 R4 EV 服务器证书 CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

数安时代 R4 EV 服务器证书 CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

数安时代 R4 OV 服务器证书 CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

数安时代 R4 OV 服务器证书 CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

数安时代 R4 IV 服务器证书 CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

数安时代 R4 IV 服务器证书 CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

数安时代 R4 DV 服务器证书 CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

数安时代 R4 DV 服务器证书 CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

数安时代 R4 代码签名证书 CA 证书将在 2030 年 12 月 31 日到期，2021 年 6 月 1 日起，已不再使用该 CA 证书签发订户证书。

数安时代 R4 代码签名证书 CA certificate will expire on December 31, 2030. As of June 1, 2021, GDCA has stopped the issuance of subscriber certificates with this CA certificate.

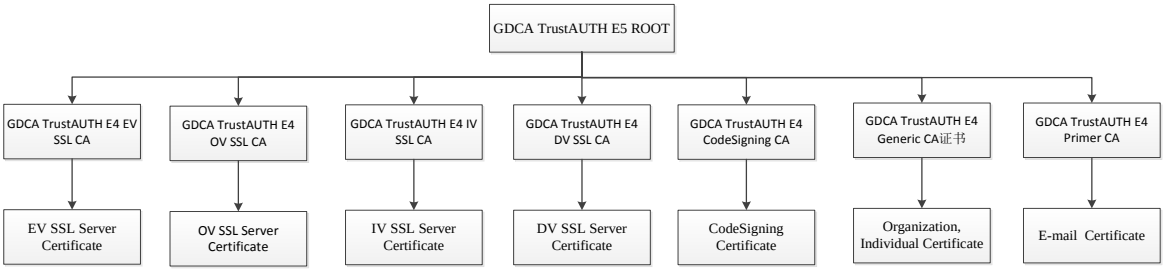
数安时代 R4 普通订户证书 CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

数安时代 R4 普通订户证书 CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

数安时代 R4 基础订户证书 CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

数安时代 R4 基础订户证书 CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

7) GDCA TrustAUTH E5 ROOT



GDCA TrustAUTH E5 ROOT 证书的密码算法为 ECC，根密钥长度为 384-bit，下设 7 个中级 CA 证书，其中：（1）GDCA TrustAUTH E4 EV SSL CA ，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 EV SSL 服务器类证书；（2）GDCA TrustAUTH E4 OV SSL CA，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 OV SSL 服务器类证书；（3）GDCA TrustAUTH E4 IV SSL CA，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 IV SSL 服务器类证书；（4）GDCA TrustAUTH E4 DV SSL CA，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 DV SSL 服务器类证书；（5）GDCA TrustAUTH E4 CodeSigning CA，密钥长度为

256-bit，签发密钥长度为 ECC 256-bit 的代码签名类证书；（6）GDCA TrustAUTH E4 Generic CA 证书，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的机构、个人类证书；（7）GDCA TrustAUTH E4 Primer CA，密钥长度为 256-bit，签发密钥长度为 ECC 256-bit 的 S/MIME 安全邮件证书。

The length of GDCA TrustAUTH E5 ROOT certificate root key is 384-bit with ECC algorithm. There are seven subordinate CAs under this ROOT CA, including: (1) GDCA TrustAUTH E4 EV SSL CA with key length of 256-bit is used for issuing 256-bit ECC EV SSL Server Certificates. (2) GDCA TrustAUTH E4 OV SSL CA with key length of 256-bit is used for issuing 256-bit ECC OV SSL Server Certificates. (3)GDCA TrustAUTH E4 IV SSL CA with key length of 256-bit is used for issuing 256-bit ECC IV SSL Server Certificates. (4) GDCA TrustAUTH E4 DV SSL CA with key length of 256-bit is used for issuing 256-bit ECC DV SSL Server Certificates. (5) GDCA TrustAUTH E4 CodeSigning CA with key length of 256-bit is used for issuing 256-bit ECC CodeSigning Certificates. (6)GDCA TrustAUTH E4 Generic CA with key length of 256-bit is used for issuing 256-bit ECC Organization, Individual Certificates. (7) GDCA TrustAUTH E4 Primer CA with key length of 256-bit is used for issuing 256-bit ECC S/MIME Certificates.

GDCA TrustAUTH E5 ROOT 证书将于 2040 年 12 月 31 日到期。

GDCA TrustAUTH E5 ROOT certificate will expire on December 31, 2040.

GDCA TrustAUTH E4 EV SSL CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH E4 EV SSL CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

GDCA TrustAUTH E4 OV SSL CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH E4 OV SSL CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

GDCA TrustAUTH E4 IV SSL CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH E4 IV SSL CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

GDCA TrustAUTH E4 DV SSL CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH E4 DV SSL CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

GDCA TrustAUTH E4 CodeSigning CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH E4 CodeSigning CA certificate will expire on December 31, 2030. From January 1,

2027, GDCA will no longer use it to issue subscriber certificates.

GDCA TrustAUTH E4 Generic CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH E4 Generic CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

GDCA TrustAUTH E4 Primer CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GDCA TrustAUTH E4 Primer CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

对于 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的订户证书：GDCA 遵循 CA/浏览器论坛（CA/Browser Forum，国际组织，又称国际 CA 浏览器联盟，是制定 CA 国际标准的机构，https://www.cabforum.org）发布的最新版本的 Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted TLS Server 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”）、Baseline Requirements for the Issuance and Management of Publicly‑Trusted S/MIME Certificate （简称“S/MIME Baseline Requirements”）及 Adobe 系统公司发布的 the Adobe Approved Trust List (AATL) Technical Requirements（简称 AATL 技术要求），进行签发和管理公共可信的 SSL/TLS 数字证书、代码签名证书、S/MIME 安全邮件证书和 Adobe 文档签名证书，定期查看其更新情况，并将持续根据其发布的版本进行修订 CP，如果本 CP 与 CA/浏览器论坛（CA/Browser Forum）发布的相关标准规范中的条款有不一致的地方，则以 CA/浏览器论坛正式发布的规范为准。

For subscriber certificates issued by the subordinate CAs which are issued by GDCA TrustAUTH R5 ROOT certificate, 数安时代R5根CA证书 and GDCA TrustAUTH E5 ROOT, GDCA conforms to the latest versions of the Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted TLS Server Certificates (hereinafter referred to as “Baseline Requirements”), Network and Certificate System Security Requirements (hereinafter referred to as “NCSSR”), Guidelines for the Issuance and Management of Extended Validation Certificates(hereinafter referred to as “EV Guidelines”), the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (hereinafter referred to as “Code Signing Baseline Requirements), Baseline Requirements for the Issuance and Management of Publicly‑Trusted S/MIME Certificate (hereinafter referred to as “S/MIME Baseline Requirements”) published by CA/Browser Forum (an international organization, also known as international CA browser alliance, to establish international standards of CA, https://www.cabforum.org), and the Adobe Approved Trust List Technical Requirements of the Adobe

Systems Inc (hereinafter referred to as “AATL Technical Requirements”) to issue and manage the publicly-trusted SSL/TLS digital certificates, publicly-trusted code signing certificates, S/MIME certificates, and Adobe PDF signing certificates. GDCA regularly checks the updates on CA/Browser Forum’s website and continually revise its CP according to these updates. The specifications of the CA/Browser Forum shall prevail in case of any discrepancies between the provisions of this CP and the standard specifications published by the CA/Browser Forum.

依据 IETF PKIX RFC 3647 CP/CPS 框架，本 CP 共分为九个章节，涵盖 GDCA 证书服务所涉及的安全控制措施，业务规则及流程。为保留 RFC3647 的整体大纲及格式，章节中含“不适用”描述的意为该章节不适用。

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CP is divided into nine parts that cover the security controls and practices and procedures for GDCA’s certificate services. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement “Not applicable”.

1.2. 文档名称与标识 Document Name and Identification

本文档称作《数安时代科技股份有限公司证书策略》（简称“《GDCA CP》”、“本 CP”）。有关本版本 CP 的修订信息请参考附录。本 CP 中为每类证书的证书策略项分配一个唯一的对象标识符，具体可参见本 CP 第 1.4.1 节。

This document is called "Global Digital Cybersecurity Authority CO., LTD. Certificate Policy" (abbreviated as “GDCA CP” or “This CP”). Please refer to Appendix for detailed revisions of this version. This CP specifies a unique object identifier for Certificate Policy of each kind of certificates (see CP section1.4.1 for details).

本 CP 以中英文双语形式发布，GDCA 应确保英文版本与中文版本无重大不一致的地方。

This document is the Chinese-English bilingual edition of GDCA CP, and GDCA should make sure that there are no material differences between the Chinese and English version.

1.3. PKI 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（Certification Authority，简称 CA）是颁发证书的实体。GDCA 是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定，依法设立的可信第三方电子认证服务机构。GDCA 通过给从事电子交易活动的各方主体颁发数字证书、提供证书验证服务等手段而成为电子认证活动的参与主体。CA 是向最终订户或其下 CA 签发证书的实体的术语，它的一个特例是根 CA，一个根 CA 是一类证书体系的最高层。

Certification Authority (abbreviated as CA) is an entity which issues certificates. GDCA is a trusted third-party electronic authentication service authority established by law based on "Electronic Signature Law of the People's Republic of China" and "Measures for the Administration of Electronic Certification Services". GDCA becomes a participant in electronic authentication activities by issuing certificates and providing certificate verification services to the parties who are engaged in electronic transaction activities. CA also means an element in certificate architecture that is issuing certificates to terminal subscribers or subordinate CAs. Root CA is a special entity, which is at the top of certificate architecture.

1.3.2. 注册机构 Registration Authorities

注册机构（Registration Authority，简称 RA）代表 CA 建立起注册过程，确认证书申请者的身份，批准或拒绝证书申请者。在订户获得证书前，它必须以申请者的身份来注册证书。证书申请者必须从 CA 或 RA 建立的注册过程来完成注册，并将注册信息提交给 CA 或 RA。CA 或 RA 将对申请者的身份及其它属性进行确认，然后决定是签发还是拒绝该请求。如果签发证书，则证书将被发送给申请者。RA 还可以根据订户需要撤销证书，尽管是 CA 完成最终的撤销工作，并将证书加入到证书撤销列表(CRL)中。

Registration Authority (RA) establishes registration process, confirms the identity of certificate applicants, and approves or rejects the request of certificate applicants on behalf of CA. Before a subscriber obtains certificate, he/she must apply for a certificate as an applicant. Certificate applicants must follow registration process established by CA or RA, and submit registration forms and related application documents to CA or RA. CA or RA will authenticate applicant's identity and other attributes, and then decide whether accept or reject this application. If CA issues the certificate, the certificate will be sent to the applicant. While RA could initiate certificate revocation process according to subscriber's requests, CA would be the only entity to complete the revocation operation and add the certificate to the certificate revocation list (CRL).

1.3.3. 订户 Subscribers

订户，即从 CA 接收证书的实体，包括所有接受 GDCA 证书的个人、单位。订户和申请人很多时候并不一致，如果订户和申请人不一致，则需要申请人保证获得明确、适当的授权。个人又分为自然人和从属于某一个单位的个人；单位包括各类政府组织、企事业单位和其它社会团体，一般而言，单位应该具有法人资格或者组织机构代码证号码；对于设备类证书，由于证书中包含主体的特殊性，订户通常应被理解为拥有该设备的单位或者个人，并由拥有该设备的单位或者个人承担相应的义务。

Subscribers, the entities that receive certificates from CA, include individuals and organizations accepting certificates from GDCA. Subscribers and applicants would not always be the same; in this case, applicants need to ensure that they have obtained explicit and appropriate authorization. Individuals can

be divided into a natural person and person who belong to an organization; Organization contains all kinds of government organizations, enterprises and institutions and other social groups. Usually, an organization has a legal personality or National Organization Code; for equipment certificates, due to the particularity of the entity contained in certificates, subscribers are usually organizations or individuals who own the equipment, and would assume the corresponding obligations.

订户代表着证书中公钥所绑定的唯一实体，拥有对与其证书唯一对应的私钥的最终控制权。订户在本 CP 的范围内使用证书，并承担本 CP 约定的义务。

Subscriber is the unique entity with corresponding public key in certificate and has ultimate rights to control corresponding private key in certificate. Subscriber should use certificates under CP restrictions, and assume the obligations agreed in this CP.

1.3.4. 依赖方 Relying Parties

依赖方是指信任证书、使用证书的个人和单位。依赖方可以是证书订户，也可以不是证书订户。

Relying parties are entities who trust and use the certificates. These entities may, or may not be a certificate subscriber.

要信任或者使用一张证书，依赖方必须验证证书的撤销信息，包括查询证书撤销列表（CRL）或使用 OCSP 方式查询证书状态。依赖方必须经过合理的审核后才能够信任一张证书。

To trust or use a certificate, a relying party must verify revocation information of the certificate by looking up the Certificate Revocation List (CRL) or searching the certificate status with OCSP servers. Before relying party trusts a certificate, a proper review process must be executed.

1.3.5. 其他参与者 Other Participants

其他参与者是指为 GDCA 的电子认证活动提供相关服务的其他实体。

Other participants are the entities that provide related services in electronic authentication activities of GDCA.

1.4. 证书应用 Certificate Usage

1.4.1. 适合的应用 Appropriate Certificate Uses

GDCA 的订户证书是通用证书，按照证书类型的不同，都有适用的应用。例如个人证书用来发送签名加密邮件、登陆办公 OA 系统等，机构证书用来进行网上申报税等，设备证书

用来标识设备身份、进行信息通道加密等。除了因为证书标识的主体身份的不同而导致证书应用差异外，GDCA 订户证书可以广泛应用在电子政务、电子商务及其他应用，以实现身份认证、电子签名、关键数据加密等目的。

Subscriber certificates of GDCA are widely used. Different types of certificate are applicable for different cases. For example, individual certificate is used for sending encrypted e-mails with digital signatures, logging into OA system, etc.; organization certificate is used for online tax declaration, etc.; and equipment certificate is used for identifying equipment and encrypting communication tunnels, etc. Apart from different applications caused by the identity of the certification subject, GDCA subscriber certificate can be widely used in e-government, e-commerce and other social activities to realize identity authentication, electronic signature, and encryption of data etc. Meanwhile, it can be used to ensure the validity and authenticity of identity between peers of communication via Internet as well as the integrity and confidentiality of information.

GDCA 订户证书，从功能上可以满足下列安全需要：

Certificates issued by GDCA can meet the following security requirements by functionalities:

- 身份真实性，保证采用 GDCA 信任服务的证书持有者身份的合法性。

- Authenticity of identity: the certification can ensure the validity of certificate holder using GDCA trust services.

- 验证信息完整性，保证采用 GDCA 数字证书和数字签名时，可以验证信息在传递过程中是否被篡改，发送和接收的信息是否一致。

- Verification of integrity: the assurance to an entity that data has not been altered and further verifies the consistency of information between sender and receiver using certificate of GDCA.

- 信息的机密性，保证传送方和接收方信息的机密性，不会泄露给其它未合法授权方。

- Confidentiality: the certification can ensure the confidentiality of information during transmission, and avoid the leakage to other non-authorized parties.

- 抗抵赖性，对信任体交易不可抵赖性的依据即数字签名进行验证。

- Non-repudiation: the certification can ensure the non-repudiation of transaction entities by verifying the digital signatures.

根据证书类型，GDCA 所签发的证书包括个人类证书、机构类证书、设备类证书、安全邮件类证书、SSL/TLS 服务器类证书、代码签名类证书等。其中：

According to the type of certificate, the certificates signed by GDCA include Individual Certificates, Organization Certificates, Equipment Certificates, S/MIME Certificates, SSL/TLS Server Certificates, and CodeSigning Certificates.

- 对于个人类证书和机构类证书，GDCA 按照所签发证书的安全等级、鉴别方式、私钥保护模式等不同，又将其分为 4 类，类别越高，安全等级越高，鉴别方式越严格；

- For Individual Certificates and Organization Certificates, GDCA classifies them into four categories according to the security level, authentication method, and private key protection mode of the

certificate. The higher the class, the higher the security level, and the more strict the authentication method;

- 对于安全邮件类证书，按照所签发证书的安全等级、鉴别方式的不同，可分为基础邮件证书、个人（IV）邮件证书、机构（OV）邮件证书和机构个人（SV）邮件证书；

- The S/MIME Certificates are categorized into three types based on the intended security levels and authentication methods, as follows: Basic S/MIME Certificates，IV S/MIME Certificates, OV S/MIME Certificates, and Sponsor-validated (SV) S/MIME Certificates;
  - 对于 SSL 服务器类证书，又分为 DV SSL（Domain Validation SSL）证书、IV SSL（Individuals Validation SSL）证书、OV SSL（Organization Validation SSL）证书和 EV SSL（Extended Validation SSL）证书；
- For SSL Server Certificates, there are DV SSL (Domain Validation SSL) Certificates, IV SSL (Individuals Validation SSL) Certificates, OV SSL (Organization Validation SSL) Certificates and EV SSL (Extended Validation SSL) Certificates;
  - 对于代码签名证书，又分为普通代码签名证书和 EV 代码签名证书；
- For CodeSigning Certificates, there are normal CodeSigning Certificates and EV CodeSigning Certificates;
  - 设备类证书、时间戳证书不再对其进行分类。
- Equipment Certificates and Timestamp Certificates have no classification.

订户可以根据实际需要，自主判断和决定采用相应合适的证书类型，不同的证书具有不同的应用范围。

Subscriber can choose suitable type of certificates based on actual requirement. Different certificates are applicable for different cases.

1.4.1.1. 个人类证书 Individual Certificates

颁发给个人的数字证书，个人包括自然人或特定身份的人员，如公务员、企业员工等。个人类证书分为以下四类（第 1 类个人证书、第 2 类个人证书不适用于 SSL/TLS 证书和代码签名证书）：

Individual certificate is a digital certificate that is issued to the individual, including natural person or personnel with specific identity, such as civil servant and employee, etc. There are four different types of individual certificates (Type I and Type II individual certificates are not applicable to SSL/TLS certificates and code signing certificates):

第 1 类个人证书——提供在网上信息传递过程中基本的认证功能，适用于低安全级别的应用领域。申请第 1 类个人证书时无需提供身份资料，GDCA 只需验证用户所提交的信息，

如邮箱地址、手机号码等，该证书应用于对安全要求不高的电子邮件签名、客户端访问控制、无需提供身份证明的小额交易等。

Type I individual certificate provides the basic authentication function in the process of online information transmission, which is applicable for the cases of the low security requirement. There is no need to offer identity information when applying for the Type I Individual Certificate. GDCA just need to verify the information submitted by users, such as e-mail address, mobile phone number and so on. Type I Individual Certificate can be used for e-mail signatures with low security requirement, client-side authentication, and small transactions that do not require any identify certificate etc.

第 2 类个人证书——提供在网上信息传递过程中的身份认证、信息加密和数字签名等功能，适用于对安全有一定要求的应用领域。申请第 2 类个人证书时需提供有限的身份资料信息，GDCA 需验证用户所提交的信息，必要时，还须通过权威第三方数据库等方式核查个人的身份信息，该证书应用于互联网认证登录、中等额度交易等。

Type II individual certificate provides the identity authentication, data encryption and digital signatures etc. in the process of online information transmission. It is applicable for the cases of the high security requirement. When applying for Type II individual certificate, GDCA requires the applicant to provide some personal information, to verify the information submitted by users and, if necessary, to authenticate the identity of the individual through an authorized third-party database. Type II Individual Certificate can be used for login through internet and the transactions with medium amount payment.

第 3 类个人证书——实现在网上信息传递过程中安全级别较高的身份认证、信息加密和数字签名等功能，适用于对安全要求较高的应用领域。申请第 3 类个人证书时需提供完整的身份信息及申请材料，GDCA 必须对身份资料及申请材料进行验证，验证的方式可以通过语音、视频、拍照等方式进行确认或将申请者提交的信息与权威第三方数据库中的信息进行比对验证，该证书应用于特定应用系统的身份认证、较大额电子商务交易等。

Type III individual certificate is used in the process of identities authentication, information encryption and digital signatures etc. during online information transmission with higher security level, applied for application areas with higher security requirement. GDCA requires the user to provide complete identity information and application materials when applying for the Type III individual certificates. The GDCA must authenticate the identity data and application materials through voices, videos, photos, etc., or compare the information with authoritative third-party database. Type III Individual Certificate can be used for the authentication of specific application system and e-commerce transactions with large amount payment.

第 4 类个人证书——实现在网上信息传递过程中安全级别最高的身份认证、信息加密和数字签名等功能，适用于对安全要求很高的应用领域。申请第 4 类个人证书时需提供完整的身份信息及申请材料，GDCA 必须通过语音、视频、拍照等或实施面对面的鉴别等方式进行确认，此外还必须将申请者提交的信息与权威第三方数据库中的信息进行比对验证，该证书应用于电子合同的签订、大额电子商务交易等。

Type IV individual certificate is used to achieve the highest security level of identity authentication, information encryption and digital signature functions during online information transmission. It is applied to the cases with highest security level. Users are required to provide complete identity information and application materials when applying for Type IV individual certificates. GDCA must verify the identity by voice, video, photograph, or face-face verification, etc.; in addition, GDCA must compare the information with an authoritative third-party database. Type IV Individual Certificate can be used for the signing of electronic contracts and large amount payment of e-commerce transactions etc.

1.4.1.2. 机构类证书 Organization Certificates

颁发给机构的数字证书，机构包括企事业单位、政府机关、社会团体等。GDCA 不签发第 1 类和第 2 类机构证书，只签发第 3 类和第 4 类机构证书：

Organization certificate is a digital certificate that is issued to organization, including enterprise, institution, government and social organization, etc. GDCA does not issue Type I and Type II Organization Certificates, and only issues Type III and Type IV Organization Certificates.

第 3 类机构证书——实现在网上信息传递过程中的身份认证、信息加密和数字签名等功能，适用于对安全要求较高的应用领域。申请第 3 类机构证书时需提供完整的身份信息及申请材料，GDCA 必须对机构证件资料及申请材料进行验证，验证的方式可以通过语音、视频、拍照等方式进行确认或将申请者提交的信息与权威第三方数据库中的信息进行比对验证，该证书应用于特定应用系统的身份认证、数字签名、加解密等。

Type III Organization Certificates are used for authentication, information encryption and digital signature in the process of information transmission on the Internet. It is applicable for the cases with high security requirements. Subscribers are required to provide complete identity information and application materials when applying for Type III Organization Certificates. GDCA must verify the identity by voices, videos, photos, face to face verification or compare the information with authorized third-party database, etc. The certificate can be used for the authentication of specific application system, digital signature, and encryption etc.

第 4 类机构证书——实现在网上信息传递过程中安全级别高的身份认证、信息加密和数字签名等功能，适用于对安全要求很高的应用领域。申请第 4 类机构证书时需提供完整的身份信息及申请材料，GDCA 必须通过语音、视频、拍照等或实施面对面的鉴别等方式进行确认，此外还必须将申请者提交的信息与权威第三方数据库中的信息进行比对验证，该证书应用于电子合同的签订、大额电子商务交易等。

Type IV Organization Certificate is used to achieve the highest security level of identity authentication, information encryption and digital signature functions during online information transmission. It can be used in the cases with highest security level. Subscribers are required to provide complete identity information and application materials when applying for a Type IV Organization Certificate. GDCA must verify the identity by voices, videos, photos, face to face verification, and compare the information with authorized third-party database. The certificates must be used with USB Key. They can be used for the

signing of electronic contracts and e-commerce transactions with large amount payment etc.

1.4.1.3. 设备类证书 Equipment Certificates

即颁发给设备的数字证书，设备包括服务器、防火墙、路由器等，此类证书通常用于网上设备的身份认证，设备之间安全信息的传递。例如，给服务器颁发的证书使浏览器可以鉴别网站服务器的身份，并创建 SSL/TLS 加密通道以使双方进行加密会话。

Equipment certificate is a digital certificate that is issued to equipment, including servers, firewalls, routers, and etc. It is usually used for network equipment identification and secure communications. For example, certificates issued to servers enable browsers to authenticate the identity of website with certificate and create SSL/TLS channel for secure session.

1.4.1.4. 安全邮件类证书 S/MIME Certificates

安全邮件证书一般适用于对电子邮件的加密和数字签名以及确保数据的安全传输，一方面可以保证邮件发送者身份真实性，另一方面保障了邮件传输过程中不被他人阅读及篡改，并由邮件接收者进行验证，确保电子邮件内容的完整性。

安全邮件证书根据类别的不同执行不同的鉴别方式：基础邮件证书只验证电子邮件地址所有权、控制权，不验证电子邮件地址所有者的真实身份；IV 邮件证书专门针对个人电子邮件地址所有权、控制权及个人电子邮件地址使用者的真实身份进行验证；OV 邮件证书除了验证电子邮件地址所有权、控制权，还会对电子邮件地址所属机构的真实身份进行验证；SV（机构个人）邮件证书，除了验证电子邮件地址所有权、控制权，还会对电子邮件地址所属机构及机构个人的真实身份进行验证。

S/MIME Certificates are generally used for encrypting and digitally signing e-mails and ensuring secure data transmissions, the certificates can ensure the authenticity of the identity of an e-mail sender and guarantee that the e-mail will not be read or tampered by an unauthorized party during the transmission, and the certificates will be verified by the recipient of the e-mail to ensure the integrity of the e-mail.

When it comes to the authentication in relation to S/MIME Certificates, GDCA follows different authentication methods based on the types of the certificates: for Basic S/MIME Certificates, GDCA only validates the ownership and control of an e-mail address and will not validate the identity of the e-mail address owner; for IV S/MIME Certificates, GDCA validates both the ownership and control of an e-mail address, and the identity of the individual who owns such e-mail address; and for OV S/MIME Certificates, GDCA validates both the ownership and control of an e-mail address, and the identity of the organization who owns such e-mail address. For Sponsor-validated (SV) S/MIME certificates, GDCA validates both ownership and control of an e-mail address, and the identity of the organization as well as the individual affiliated to the organization who owns such e-mail address.

1.4.1.5. SSL 服务器类证书 SSL Server Certificates

SSL/TLS 服务器类证书标识 Web 网站或者 Web 服务器的身份，可以用于证明网站的身份或者资质、提供 SSL/TLS 加密通道，不得用于各类交易、支付的签名或验证。

SSL/TLS server certificate is a digital certificate that identifies the website or server, applicable for verification of website certificates and provides SSL/TLS channel. It cannot be used for signature or verification of transaction and payment.

GDCA 所签发的 SSL 服务器类证书包括以下四种：

SSL server certificates of GDCA include the following:

- EV SSL 证书（Extended Validation SSL Certificates），即扩展验证型服务器证书
- EV SSL certificate (Extended Validation SSL Certificates), the extended validation SSL certificates.
- OV SSL 证书（Organization Validation Certificates），即需要验证网站所有机构真实身份的标准型 SSL 证书
- OV SSL certificate (Organization Validation Certificates), the SSL certificate requires to verify the identity of the organization that owns the website.
- IV SSL 证书（Individuals Validation SSL Certificates），即需要验证网站经营者个人身份的标准型 SSL 证书
- IV SSL certificate (Individuals Validation SSL Certificates), the SSL certificate requires to verify the individual identity of website owner.
- DV SSL 证书（Domain Validation SSL Certificates），即只验证网站域名所有权的简易型 SSL 证书
- DV SSL certificate (Domain Validation SSL Certificates), the SSL certificate that only verifies the ownership of the website.

其中，OV SSL 证书、IV SSL 证书可实现网站机密信息的加密以及网站身份的验证功能，DV SSL 证书只提供网站机密信息的加密功能。EV SSL 证书遵循《GDCA EV 证书策略》，本 CP 不再对其进行具体阐述。

OV SSL certificate and IV SSL certificate provide the functions of information encryption and verification of website identity. DV SSL certificate only provides information encryption. The issuance and usage of EV SSL certificate conforms to “GDCA EV CP”, which is no longer covered in this CP.

SSL 服务器证书不限制域名的种类，如商业域名、政府域名等。

The types of domain names in SSL/TLS server certificates are not restricted, e.g. .com, .gov etc.

1.4.1.6. 代码签名类证书 CodeSigning Certificates

代码签名类证书标识软件代码的来源或者所有者，只能用于各类代码的数字签名，不得用于各类交易、支付、加密等应用。

CodeSigning certificate is a digital certificate that identifies the source or owner of the software code. It can only be used for digital signature and cannot be used for transaction, payment and encryption, etc.

代码签名类证书订户必须承诺，不得将代码签名类证书用于对恶意软件、病毒代码、侵权软件、黑客软件等的签名。

Subscriber must commit not to sign malicious software, virus code, infringement software and hacker software using CodeSigning certificate.

1.4.1.7. 时间戳类证书 TimeStamp Certificates

时间戳证书主要用于时间戳服务器，提供数字签名功能。

Timestamp Certificates are mainly used for Timestamp servers to provide digital signature service.

1.4.1.8. 各类证书的证书策略对象标识符 CP Object Identifiers of Certificates

在本 CP 中为每类证书的证书策略项分配一个唯一的对象标识符，具体如下：

We assign a unique object identifier to certificate policy items of different types in this CP, the regulation is as follows:

对于由 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2）、GDCA ROOT CA1 证书签发的中级 CA 所签发的用户证书，证书策略标识符（OID）如下：

第 1 类个人证书策略: 1.2.156.112559.1.2.1.1

第 2 类个人证书策略: 1.2.156.112559.1.2.1.2

第 3 类个人证书策略: 1.2.156.112559.1.2.1.3

第 4 类个人证书策略: 1.2.156.112559.1.2.1.4

第 3 类机构证书策略: 1.2.156.112559.1.2.2.1

第 4 类机构证书策略: 1.2.156.112559.1.2.2.2

设备证书策略: 1.2.156.112559.1.2.3.1

测试用途证书策略 ： 1.2.156.112559.1.99.1.1

For the subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, the allocated policy OIDs are as follows:

Type I individual certificate policy: (1.2.156.112559.1.2.1.1)

Type II individual certificate policy: (1.2.156.112559.1.2.1.2)

Type III individual certificate policy: (1.2.156.112559.1.2.1.3)

Type IV individual certificate policy: (1.2.156.112559.1.2.1.4)

Type III organization certificate policy: (1.2.156.112559.1.2.2.1)

Type IV organization certificate policy: (1.2.156.112559.1.2.2.2)

Equipment certificate policy: (1.2.156.112559.1.2.3.1)

Certificates for test purpose: (1.2.156.112559.1.99.1.1)

对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的用户证书，证书策略（OID）及密钥用法如下：

证书类别	策略对象标识符	密钥用法	备注
邮件证书（原个人 1 类证书）	1.2.156.112559.1.1.1.1	密钥用法：数字签名，密钥加密，数据加密。 增强型密钥用法：客户端身份验证，电子邮件保护。	2022 年 11 月 1 日起不再用于安全邮件证书。
Adobe 文档签名证书	1.2.156.112559.1.1.1.2	密钥用法：数字签名，不可否认； 增强型密钥用法：Adobe 文档签名。	
机构个人邮件证书	1.2.156.112559.1.1.2.4 2.23.140.1.5.3.2	密钥用法：数字签名，密钥加密，数据加密。 增强型密钥用法：客户端身份验证，电子邮件保护。	
机构邮件证书	1.2.156.112559.1.1.2.1 2.23.140.1.5.2.2	密钥用法：数字签名，密钥加密，数据加密。 增强型密钥用法：客户端身份验证，电子邮件保护。	
个人邮件证书	1.2.156.112559.1.1.2.2 2.23.140.1.5.4.2	密钥用法：数字签名，密钥加密，数据加密。 增强型密钥用法：客户端身份验证，电子邮件保护。	
基础邮件证书	1.2.156.112559.1.1.2.3 2.23.140.1.5.1.2	密钥用法：数字签名，密钥加密，数据加密。 增强型密钥用法：客户端身份验证，电子邮件保护。	
DV SSL 证书	1.2.156.112559.1.1.4.3 及 2.23.140.1.2.1	密钥用法：数字签名， 密钥加密。 增强型密钥用法：客户端身份验证 ，服务器身份验证。	
OV SSL 证书	1.2.156.112559.1.1.4.1 及 2.23.140.1.2.2	密钥用法：数字签名， 密钥加密。 增强型密钥用法：客户端身份验证 ，服务器身份验证。	
IV SSL 证书	1.2.156.112559.1.1.4.2 及 2.23.140.1.2.3	密钥用法：数字签名， 密钥加密。 增强型密钥用法：客户端身份验证 ，服务器身份验证。	

EV SSL 证书	1.2.156.112559.1.1.6.1 及 2.23.140.1.1	密钥用法：数字签名， 密钥加密。 增强型密钥用法：客户端身份验证 ，服务器身份验证。	
普通代码签名类证书	1.2.156.112559.1.1.5.1	密钥用法：数字签名。 增强型密钥用法：代码签名。	
EV 代码签名证书	1.2.156.112559.1.1.7.1 及 2.23.140.1.3	密钥用法：数字签名。 增强型密钥用法：代码签名。	
时间戳证书	1.2.156.112559.1.1.8.1	密钥用法：数字签名。 增强型密钥用法：时间戳。	

For the subscriber certificates issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT, 数安时代 R5 根 CA 证书, and GDCA TrustAUTH E5 ROOT, the allocated policy OIDs are as follows:

Types of Certificates	Policy OIDs	Key Usages	Remarks
Email Certificates (Previously the Type I Individual Certificates)	1.2.156.112559.1.1.1.1	KU: Digital Signature, Key Encipherment. EKU: Client Authentication, Email Protection.	This policy OID will not be used to identify the email certificates as of 1 November 2022.
Adobe PDF signing certificates	1.2.156.112559.1.1.1.2	KU: Digital Signature, Non Repudiation. EKU: Adobe Document Signing.	
SV S/MIME Certificates	1.2.156.112559.1.1.2.4 2.23.140.1.5.3.2	KU: Digital Signature, Key Encipherment, Data Encipherment. EKU: Client Authentication, Email Protection.	
OV S/MIME Certificates	1.2.156.112559.1.1.2.1 2.23.140.1.5.2.2	KU: Digital Signature, Key Encipherment, Data Encipherment. EKU: Client Authentication, Email Protection.	
IV S/MIME Certificates	1.2.156.112559.1.1.2.2 2.23.140.1.5.4.2	KU: Digital Signature, Key Encipherment, Data Encipherment. EKU: Client Authentication, Email Protection.	
Basic S/MIME Certificates	1.2.156.112559.1.1.2.3	KU: Digital Signature, Key Encipherment, Data	

	2.23.140.1.5.1.2	Encipherment. EKU: Client Authentication, Email Protection.	
DV SSL Certificates	1.2.156.112559.1.1.4.3 and 2.23.140.1.2.1	KU: Digital Signature, Key Encipherment. EKU: Client Authentication, Server Authentication.	
OV SSL Certificates	1.2.156.112559.1.1.4.1 and 2.23.140.1.2.2	KU: Digital Signature, Key Encipherment. EKU: Client Authentication, Server Authentication.	
IV SSL Certificates	1.2.156.112559.1.1.4.2 and 2.23.140.1.2.3	KU: Digital Signature, Key Encipherment. EKU: Client Authentication, Server Authentication.	
EV SSL Certificates	1.2.156.112559.1.1.6.1 and 2.23.140.1.1	KU: Digital Signature, Key Encipherment. EKU: Client Authentication, Server Authentication.	
Standard Code Signing Certificates	1.2.156.112559.1.1.5.1	KU: Digital Signature. EKU: Code Signing.	
EV Code Signing Certificates	1.2.156.112559.1.1.7.1 and 2.23.140.1.3	KU: Digital Signature. EKU: Code Signing.	
TimeStamp Certificates	1.2.156.112559.1.1.8.1	KU: Digital Signature. EKU: Time Stamping.	

1.4.2. 限制的证书应用 Prohibited Certificate Uses

一般而言，GDCA 证书是一般性目的的证书，可以和不同的依赖方之间相互操作。尽管如此，GDCA 证书在功能上是受到限制的，如个人证书只能用于个人用户的应用，而不能作为服务器或机构证书使用。与应用类型不一致的证书，不应被本 CP 识别为可信任。

In general, GDCA certificates are general certificates. These certificates can be used among different relying parties for mutual operations. However, some features of the certificates are prohibited. For example, the Individual Certificate can only be used as individual case rather than the cases being used as Equipment or Organization Certificate. Certificates shall not be deemed as trusted by this CP if they

are not corresponding to their respective usages.

禁止在任何违反国家法律、法规或破坏国家安全的情形下使用证书，也禁止在任何违法犯罪活动或法律禁止的相关业务下使用证书，否则由此造成的法律后果由用户自己承担。

The certificate is prohibited to be used in such circumstances, such as any violation of state laws, regulations and national security or legal consequences, in addition, a certificate is prohibited to be used in business that involves criminal activities, or in business forbidden by laws, otherwise all legal liability that triggered by this will be taken consciously by user themselves.

ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 可用于测试订户证书的签发。测试证书仅供用户测试使用，GDCA 对测试证书的真实性、有效性及其在测试以外场景中的使用后果不承担任何责任。GDCA 强烈建议用户不得将测试证书用于除测试以外的任何用途，特别是不得用于涉及真实身份验证的应用场景，以避免可能产生的损失或纠纷。

为确保测试证书的可识别性和管理规范性，GDCA 测试证书用户名中必须含英文“test”或者中文“测试”字样，且证书有效期最长不超过 6 个月。

Subordinate CA Certificates issued under the ROOTCA (RSA) Certificate, GDCA ROOT CA Certificate, ROOTCA (SM2) Certificate, and GDCA ROOT CA1 Certificate may be used for issuing test subscriber certificates. Test certificates are provided solely for testing purposes, and GDCA assumes no responsibility for the authenticity, validity, or any consequences arising from the use of test certificates outside testing environments. GDCA strongly advises users not to use test certificates for any purposes other than testing, especially in scenarios involving identity verification, in order to avoid potential losses or disputes.

To ensure the identifiability and proper management of test certificates, GDCA requires that the username in each test certificate must contain the English word “test” or the Chinese word “测试”, and that the validity period of these certificates shall not exceed six months.

1.5. 策略管理 Policy Administration

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

GDCA 安全策略委员会是 GDCA 电子认证服务所有策略的最高管理机构，负责制定、维护和解释本 CP。

GDCA Security Policy Committee is the highest management authority responsible for review and approval of electronic certificate services, as well as the highest decision organization to perform inspection and supervision of the CP.

GDCA 安全策略委员会由来自于公司管理层、行政中心、技术中心、客户服务中心等拥有决策权的合适代表组成。

GDCA Security Policy Committee is assigned as the document management authority responsible for establishing, publishing and updating this CP. The committee consists of the relevant representatives with the right of decision-making from GDCA's management, administrative center, technology center, and customer service center, etc.

GDCA 安全策略委员会的所有成员在就证书策略进行管理和批准时，均享有一票决定权，如果选票相同，委员会主任可拥有双票决定权。

Member of GDCA Security Policy Management Committee has the right to vote over management and approval of certificate policy. The Chairman of the committee may have two votes for decision in case of tie of votes.

本策略文档的对外咨询服务等日常工作由行政管理部门负责。

Consultation of this policy document to the external parties and other routine jobs are undertaken by the administrative center.

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之一提交，且证书撤销请求必须以书面形式提交：

- 发邮件至：webtrustreport@gdca.com.cn；或
- 致电：4007008088

Any certificate problem reports or certificate revocation requests shall be submitted through one of the following ways and certificate revocation requests must be submitted in writing:

- E-mail to: webtrustreport@gdca.com.cn
- Call: 4007008088

1.5.2.2. CPS 问题 CPS Related Issues

联系部门：GDCA 行政管理部门

Contact Department: GDCA Administrative Department

联系人：王女士

Contact: Ms. Wang

邮件地址：gdca@gdca.com.cn

E-mail: gdca@gdca.com.cn

联系电话：+86 20-83487228

Tel: +86 20-83487228

地址：中华人民共和国广东省广州市越秀区越华路 112 号珠江国际大厦 30 楼 3001 室

Address: Unit 3001, 30F, Pearl River International Building, No. 112 Yuehua Road, Yuexiu District, Guangzhou City, Guangdong Province, the People's Republic of China

邮编：510030

Postal Code: 510030

1.5.3. 决定 CP 符合策略的机构 Person Determining CP Suitability for the Policy

本 CP 由 GDCA 安全策略委员会批准，包括本 CP 的修订和版本变更。

This CP and the corresponding revisions and version changes should be approved by the GDCA Security Policy Committee.

GDCA 安全策略委员会负责评估 GDCA 的 CPS 是否符合本 CP，是批准和决定 GDCA 的 CPS 是否与本 CP 相适应的机构。

GDCA Security Policy Committee is responsible for assessing whether GDCA CPS is in accordance with this CP as well as approving and deciding whether the CPS of GDCA corresponds with the CP or not.

1.5.4. CP 批准程序 CP Approval Procedures

本 CP 由 GDCA 安全策略委员会组织相关人员拟定文档，提交 GDCA 安全策略委员会批准审核。

This CP is drafted by relevant personnel organized by the GDCA Security Policy Committee and submitted to the GDCA Security Policy Committee for review and approval.

1.5.5. CP 修订 CP Revision

GDCA 将对 CP 进行严格的版本控制，并由安全策略委员会负责相关事宜。

GDCA 根据国家的政策法规、技术要求、标准的变化及业务发展情况及时修订本 CP，同时对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的公共可信证书业务，GDCA 还根据 CA/B 论坛（https://www.cabforum.org.）发布的最新版本的 Baseline Requirements、EV Guidelines、Code Signing Baseline Requirements、S/MIME Baseline Requirements 及 NCSSR 的要求及时修订 CP。

CP 编写小组根据相关的情况拟定 CP 修订建议，提交 GDCA 安全策略委员会审核，经该委员会批准后，正式在 GDCA 官方网站上发布。

本 CP 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。

GDCA will implement strict version controls on this CP, and such work will be arranged by the GDCA Security Policy Committee.

This CP will be updated timely in line with the changes of national policies and regulations, technical requirements, standards and business development. Meanwhile, for the publicly trusted certificates issued by the subordinate CAs that are issued by GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA 证书 and GDCA TrustAUTH E5 ROOT, GDCA shall also update this CP according to the latest versions of the Baseline Requirements, the EV Guidelines, the Code Signing Baseline Requirements, S/MIME Baseline Requirements and the NCSSR of the CA/B Forum (https://www.cabforum.org).

This CP is updated at least once every year. Even if no other changes are made to the contents of this CP, GDCA will increment the version number and update the release date, effective date, and the revision records of this CP.

1.6. 定义和缩写 Definitions and Acronyms

1.6.1. 术语定义一览表 List of Term Definition

术语	定义
GDCA 安全策略委员会	GDCA 认证服务体系内的最高策略管理监督机构和 CP 一致性决定机构
电子认证服务机构	负责建立，签发，撤销及管理证书的某个机构。该术语适用于根 CAs 及中级 CAs。
注册机构	注册机构（Registration Authority，RA）负责处理证书申请者和证书订户的服务请求，并将之提交给认证服务机构，为最终证书申请者建立注册过程的实体，负责对证书申请者进行身份标识和鉴别，发起或传递证书撤销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。
证书	使用数字签名的电子文件，用于将公钥与身份绑定。
证书撤销列表	由签发证书的电子认证服务机构（CA）创建并进行数字签名，且定期更新的已撤销证书的带时间戳列表。
电子认证业务规则	构成证书建立，签发，管理及使用管理框架的一份文件。
域名	域名系统中分配至某个节点的标签。
完全限定域名	包括互联网域名系统中所有高级节点标签的域名。
Linting 检测	一种对数字签名数据内容，如预证书（RFC 6962）、证书、证书吊销列表或 OCSP 响应，或待签名数据对象（RFC 5280 第 4.1.1.1 节所述的 tbsCertificate）进行检查的过程，以确保其符合基线要求中定义的配置文件和标准。
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。
私钥	由密钥对持有者严格保密的密钥对中的密钥，用于创建数字

	签名，及/或解密通过相应公钥加密的电子记录或文件。
公钥	密钥对中可由相应私钥持有者公开的密钥，可被某个依赖方使用，以核实与持有人相应私钥一并创建的数字签名，及/或可用于加密信息，以便仅相应私钥持有者可对此类信息进行解密。
公钥基础设施	一组包括硬件、软件、人员、流程、规则及责任的合集，用于实现基于公钥密码的密钥及证书的可信创建、签发、管理及使用的功能。
公共可信证书	由于其相应的根证书以信任锚的形式在广泛可用的应用软件中部署，从而可信的证书。
合格的审计师	符合本 CP 章节 8.2 所述要求的自然人或法律实体。
依赖方	依赖某有效证书的自然人或法律实体。
订户	被签发证书的自然人或法律实体，且受订户协议或使用条款约束的自然人或法律实体。
订户协议	认证服务机构与证书申请人/订户之间的协议，该协议规定了各方的权力与责任。
WebTrust	CPA 加拿大针对认证服务机构的 WebTrust 项目的现行标准。

Term	Definition
GDCA Security Policy Committee	It is the highest management and monitor function for CPS and the decision-making agency pursuant to CP within the GDCA certification services system.
Certification Authority	An organization that is responsible for the creation, issuance, revocation, and management of certificates. The term applies equally to both Roots CAs and Subordinate CAs.
Registration Authority	A Registration Authority (RA) is responsible for processing service requests from certificate applicants and certificate subscribers, and submitting them to the certification authority for the final certificate applicant to establish registration process. RA is also responsible for identifying and verifying certificate applicants, initiating or transferring certificate revocation request, and approving certificate renewal or re-key request on behalf of the certification authority.
Certificate	An electronic document that uses a digital signature to bind a public key and an identity.
Certificate Revocation List	A regularly updated time-stamped list of revoked certificates that is created and digitally signed by the CA that issued the certificates.
Certification Practice Statement	One of several documents forming the governance framework in which certificates are created, issued, managed, and used.
Domain Name	The label assigned to a node in the Domain Name System.
Fully Qualified Domain	A Domain Name that includes the labels of all superior nodes in the

Name	Internet Domain Name System.
Linting	A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-besigned object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in the Baseline Requirements.
Online Certificate Status Protocol	An online certificate-checking protocol that enables relying party application software to determine the status of an identified certificate.
Private Key	The key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding public key.
Public Key	The key of a key pair that may be publicly disclosed by the holder of the corresponding private key and that is used by a relying party to verify digital signatures created with the holder's corresponding private key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding private key.
Public Key Infrastructure	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of certificates and keys based on public key cryptography.
Publicly Trusted Certificate	A certificate that is trusted by virtue of the fact that its corresponding root certificate is distributed as a trust anchor in widely-available application software.
Qualified Auditor	A natural person or legal entity that meets the requirements of section 8.2 of this CP.
Relying Party	Any natural person or legal entity that relies on a valid certificate.
Subscriber	A natural person or legal entity to whom a certificate is issued and who is legally bound by a subscriber agreement.
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
WebTrust	The current version of CPA Canada’s WebTrust Program for Certification Authorities

1.6.2. 缩略语及其含义一览表 List of Abbreviations and their Meaning

CA	Certification/Certificate Authority	电子认证服务机构

CAA	Certification Authority Authorization	认证机构授权
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则
CRL	Certificate Revocation List	证书撤消列表
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
EV	Extended Validation	扩展验证/增强验证
FIPS	(US Government) Federal Information Processing Standard	（美国政府）联邦信息处理标准
FQDN	Fully Qualified Domain Name	完全限定域名
GDCA	Global Digital Cybersecurity Authority CO., LTD.	数安时代科技股份有限公司
gTLD	Generic Top-Level Domain	通用顶级域名
IANA	Internet Assigned Numbers Authority	互联网编码分配机构
ICANN	Internet Corporation for Assigned Names and Numbers	互联网名字与编号分配机构
ISO	International Organization for Standardization	国际标准化组织
KM	Key Management	密钥管理
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
LRA	Local Registration Authority	本地注册机构
OCSP	Online Certificate Status Protocol	在线证书状态协议
OSCCA	State Cryptography Administration Office of Security Commercial Code Administration of China	中国国家商用密码管理办公室
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	公钥基础设施
RA	Registration Authority	注册机构
RFC	Request For Comments	请求评注标准(一种互联

		网建议标准)
SSL	Secure Sockets Layer	安全套接字
TLS	Transport Layer Security	传输层安全
AATL	Adobe Approved Trust List	Adobe 批准信任列表

2. 发布与信息库责任 Publication and Repository Responsibilities

2.1. 信息库 Repositories

GDCA 信息库是一个对外公开的信息库，它能够保存、取回证书及与证书有关的信息。GDCA 信息库内容包括但不限于以下内容：CP 和 CPS 现行和历史版本、证书、CRL、订户协议，以及其它由 GDCA 在必要时发布的信息。GDCA 将及时发布包括证书、CPS 修订和其它资料等内容。GDCA 信息库可以通过网址：https://www.gdca.com.cn 查询，或由 GDCA 随时指定的其它通讯方法获得。

GDCA repositories are open to the public. It can store, retrieve certificates and their related information. GDCA repository includes but not limited to the following: current and historical CPs and CPSs, certificates, CRLs, subscriber agreements and other information published by GDCA when necessary. GDCA will release certificates, CP and CPS revisions and so on timely that must remain consistent with the CPS, relevant laws and regulations. You can search at https://www.gdca.com.cn or via any other communication methods specified by GDCA at any time.

2.2. 信息的发布 Publication of Certification Information

GDCA 在官方网站 https://www.gdca.com.cn 发布信息库，该网站是 GDCA 发布所有信息最首要、最及时、最权威的渠道。

GDCA publishes repositories on its official website (https://www.gdca.com.cn). The official website is the primary, most prompt and authoritative channel to publish all information about GDCA.

GDCA 通过目录服务器发布订户的证书和 CRL，订户或依赖方可以通过访问 GDCA 的官网获取证书的信息和撤销证书列表；同时，GDCA 提供在线证书状态查询服务，订户或依赖方可实时查询证书的状态信息。

GDCA publishes certificates and CRLs via LDAP. Subscriber or relying party can obtain information of certificates and CRLs through GDCA's official website. Meanwhile, subscriber or relying party can get the current status of certificate instantly via OCSP service provided by GDCA.

同时，GDCA 也将会根据需要采取其他可能的形式进行信息发布。

Meanwhile, GDCA may also release any related information in other possible forms.

2.3. 发布的时间和频率 Time or Frequency of Publication

GDCA 在订户证书签发或者注销时，通过官方网站自动将证书和 CRL 发布。

对于由 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 所签发的订户证书，CRL 发布周期为 8 小时。

对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的订户证书，CRL 发布周期为 24 小时，且 nextUpdate 字段的值不超出 thisUpdate 值的 10 天以上。

在紧急的情况下，GDCA 可以自行决定证书和 CRL 的发布时间。GDCA 每年发布一次电子认证服务机构的 CA 证书撤销列表（ARL）。

GDCA releases automatically the latest certificates and CRLs via its official website when the certificates are issued or revoked.

The subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, the CRLs are issued every 8 hours.

For the subscriber certificates issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT, 数安时代 R5 根 CA 证书, and GDCA TrustAUTH E5 ROOT, the CRLs are issued every 24 hours and the value of the nextUpdate field is not more than ten days beyond the value of the thisUpdate field.

In particular, GDCA can choose time to release the certificates and CRL in case of an emergency. GDCA releases CRL of CA (ARL) every year.

信息库其他内容的发布时间和频率，由 GDCA 独立做出决定，这种发布应该是及时的、高效的，并且是符合国家法律的要求的。

GDCA can individually choose the time and frequency of releasing other information of repository. The release is efficient, timely and consistent with the requirements of the laws.

2.4. 信息库访问控制 Access Controls on Repositories

GDCA 信息库中的信息是对外公开发布的，任何人都能够查阅，对这些信息的只读访问不受任何限制。

GDCA 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进行信息库的增加、删除、修改、发布等操作。

The information in GDCA repository is publicly available. Anybody can read the relevant information, and

there are no restrictions on the read-only access of such information.

With network security, secure system design and security policy, GDCA ensures that only authorized employees can add, delete, modify and publish the repositories.

3. 身份标识与鉴别 Identification and Authentication

3.1. 命名 Naming

3.1.1. 命名类型 Types of Names

GDCA 签发的数字证书符合 X.509 标准，分配给证书持有者的主体甄别名，采用 X.500 命名方式。

The certificate issued by GDCA format meets X.509 standard and the identifier which is assigned to the subscriber as the DN meets X.500 standard.

对于 SSL/TLS 服务器证书，所有的域名都添加到主题别名中，而主题通用名为主域名，必须包含一个出现在主题别名中的全域名或 IP 地址。

For SSL/TLS server certificate, all domain names or IP addresses are added as the Subject Alternative Name and the common name is a primary domain name which must be one of the domain names or IP addresses from the Subject Alternative Name.

3.1.2. 对命名有意义的要求 Need for Names to be Meaningful

订户证书所包含的命名应具有一定的代表性意义，可以确定证书主题中的个人、机构或者设备的身份。

The subscriber’s name must be meaningful, usually contains the semantics which could be understood. The name could be used to confirm the identity of individuals, organizations or equipment in the certificate subjects.

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

订户不能使用匿名、伪名申请证书，证书中也不能使用匿名、伪名。

Subscribers cannot use anonymous or pseudonyms to apply for certification. Also, anonymous or pseudonyms cannot be used in certificates.

3.1.4. 解释不同命名的规则 Rules for Interpreting Various Name Forms

依 X.500 甄别名命名规则解释。

The interpretation should conform to naming rules of X.500 DN.

3.1.5. 命名的唯一性 Uniqueness of Names

GDCA 应保证签发给某个订户的证书，其主体甄别名，在 GDCA 信任域内是唯一的。当出现相同的名称时，以先申请者优先使用。

DN of certificate must be unique for different subscribers in GDCA trust domain. When DN is not unique to different subscribers, the first applicant of this DN shall govern.

3.1.6. 商标的识别、鉴别与角色 Recognition, Authentication, and Role of Trademarks

GDCA 签发的证书的主体甄别名中不包含商标名。

Subject's DN of certificate issued by GDCA does not contain any trademarks.

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要注册公钥相对应的私钥，证明的方法包括在证书申请消息中包含数字签名（PKCS#10）、其它与此相当的密钥标识方法，或者 GDCA 要求的其它证明方式，包括提交的初始化信息（被分配的密钥存储介质和对应的 PIN 码）等。

Applicants must prove that he/she holds the corresponding private key to the public key being registered. You can use the ways of digital signature contained in certificate request messages (PKCS#10) or other equivalent method to identify the secret keys, or some ways required by GDCA, such as initial information (distributed key medium and its PIN code), etc. to prove that you holds the relevant keys.

3.2.2. 个人身份的鉴别 Authentication of Individual Identity

个人身份的鉴别包括如下内容：

Authentication of individual identity includes the following:

1. 鉴别证明包括但不限于个人身份证或军官证等由政府机构颁发的能够证明个人身份的有效文件，或者通过签发有效文件的权威第三方数据库确认。

1. Authentication attestation includes but is not limited to valid government issued personal ID or military ID, or valid authoritative third-party database signed document.

2. 核查证书申请关键信息与有效文件或第三方数据库的资料是否相符，避免信息填写

有误，但注册信息最终以申请者确认为准。

2. GDCA verifies to a reasonable level of assurance that key information in certificate application matches valid document or third-party database. But final confirmation of applicant's information shall govern.

3. 订户可采用面对面或者邮政信函等方式提交政府机构签发的有效文件。

3. Subscribers can submit valid government issued document through methods such as face-to-face submission or postal mail.

4. 对于以某个组织中的个人身份名义申请的，还需要提交其所在单位提供的证明材料。

4. If an applicant belongs to an organization and applied on his/her own, relevant attestation from his/her organization should also be provided.

5. 确认经办人是否得到足够的授权，确认的方式可以是：订户授权给经办人申请办理证书事宜的授权文件及经办人有效身份证件的原件或者复印件。

5. GDCA authenticates the representative's authority to represent the applicant by checking authorized document from applicant and valid original and copy of personal ID.

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。

If the request contains organization information, GDCA should confirm the existence of this organization and the applicant belongs to the organization.

GDCA 必须根据个人所申请的证书类别的不同，执行不同的身份鉴别方式，一般而言，证书类别越高，安全等级越高，鉴别方式越严格，鉴别内容越全面。第 1 类个人证书及第 2 类个人证书不适用于 SSL/TLS 证书和代码签名证书。

GDCA must perform different authentication methods depending upon the type of certificate applied by the individual. Generally, the higher class certificate type means higher security level, and stricter authentication method with more comprehensive authentication information. Type I and Type II individual certificates are not applicable to SSL/TLS certificates and code signing certificates.

1. 对于第 1 类个人证书，执行以下鉴别：

1. For Type I Individual Certificate, the following authentication is performed:

GDCA 只需验证用户所提交的信息，不对订户的通用名进行验证。确认的方式可以采用发送相关校验码或通过电话、手机短信等其他可靠的方式来实现对申请者所提交的信息的鉴别和验证。GDCA 不确认、不担保所签发的证书中除验证信息以外的其他身份信息是真实的、可靠的、属于申请者本人的。

GDCA only verifies the information submitted by the subscriber and does not validate the identity of the subscriber. The information submitted by the subscriber can be validated by sending a verification code, making a phone call, sending an SMS message or any other reasonable ways. GDCA will not ensure or guarantee the validation and reliance of other information, and will not validate whether the information

belongs to the subscriber, except the information submitted by the subscriber.

2. 对于第 2 类个人证书，执行以下鉴别：

2. For the Type II Individual Certificate, the following authentication is performed:

GDCA 需验证用户所提交的信息，证书中的通用名为订户的真实姓名。确认的方式可以是通过采用发送相关校验码或通过电话、手机短信等其他可靠的方式来验证申请者所提供的信息的真实性，必要时，还需通过查询权威第三方数据库等可靠的方式对申请者提供的身份信息进行核实验证，确保申请者所提供的信息与核查结果一致。

GDCA shall verify the information submitted by the subscriber, and to verify that the common name is the real name of the subscriber. The information submitted by the subscriber can be validated through sending a verification code, making a phone call, sending an SMS message or any other reasonable ways. GDCA can also validate the identity of the subscriber through the well-known third-party database if necessary, to ensure the consistency of the information from different channels.

3. 对于第 3 类个人证书，执行以下鉴别：

3. For the Type III Individual Certificate, the following authentication is performed:

1) 确认申请者身份的真实性和有效性。确认的方式必须是获得申请者至少一种由政府机构颁发的、有效的、带照片的身份证明文件（如居民身份证、护照、军官证或其他同等证照），GDCA 检查该证明文件是否有任何篡改或伪造的痕迹，必要时，GDCA 可以通过签发有效身份证明文件的权威第三方数据库进行核查确认申请者身份，也可以通过语音通话、视频、拍照等方式对申请者提供的信息进行核实验证，确保所提供的信息与核查结果一致。

1) Ensure the identity of the subscriber. This must be validated by obtaining at least one currently valid government-issued photo ID (e.g. ID card, passport, military ID, or equivalent document type), GDCA shall inspect the copy for any indication of alteration or falsification. GDCA cross-checks with an authoritative third-party database that issues the valid identification document, when necessary, GDCA may also verify the information submitted by the subscriber through a voice communication, video, photo taking, etc. as well as validate through cross-checking with a well-known third-party database, to ensure the consistency of the information from different channels.

2) 确认申请者的地址。GDCA 可以通过物业费账单、银行卡账单或信用卡账单等核实申请者的地址或直接依赖政府签发的身份证明文件上的地址。

2) GDCA may verify the address of the applicant using a utility bill, bank statement, credit card statement etc., or directly rely on the address on the identification document issued by the government.

3) 核查证书请求的真实性。GDCA 通过电话、邮件等方式，与申请者核实证书请求。

3) GDCA verifies the certificate request with the applicant by sending e-mails or making phone calls etc.

4) 对于以某个组织中的个人身份名义申请的，还需要提交其所在单位提供的证明材料。

4) For the application applied by someone in his/her name who works in an organization, the applicant also needs to provide the proof materials from the organization.

5) 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。如要求查询第三方数据库、发送确认电子邮件等。

5) When the application information contains some information of an organization, it is necessary to confirm the existence of the organization and whether the applicant belongs to the organization. GDCA could require validating by a third-party database, or sending e-mails to the organization, and so on.

4. 对于第 4 类个人证书，执行以下鉴别：

4. For the Type IV Individual Certificate, the following authentication is performed:

1) 确认申请者身份的真实性和有效性 。确认的方式同时包括：1）必须是获得申请者至少一种由政府机构颁发的、有效的、带照片的身份证明文件（如居民身份证、护照、军官证或其他同等证照），GDCA 检查该证明文件是否有任何篡改或伪造的痕迹；2）通过签发有效身份证明文件的权威第三方数据库进行核查确认，确保所提供的信息与核查结果一致。

1) Ensure the identity of the subscriber. Ways of authentication are: 1) obtaining at least one currently valid government-issued photo ID (e.g. ID card, passport, military ID, or equivalent document type), GDCA will inspect the copy for any indication of alteration or falsification; and 2) Cross-checking with an authoritative third-party database that issues the valid identification document, to ensure the consistency of the information from different channels.

2) 确认申请者的地址。GDCA 可以通过物业费账单、银行卡账单或信用卡账单等核实申请者的地址或直接依赖政府签发的身份证明文件上的地址。

2) GDCA may verify the address of the applicant using a utility bill, bank statement, credit card statement etc., or directly rely on the address on the identification document issued by the government.

3) 核查证书请求的真实性。GDCA 通过电话、邮件等方式，与申请者核实证书请求。

3) GDCA should verify the certificate request with the applicant by sending e-mails or making phone calls etc.

4) 必要时，GDCA 可以通过语音通话、视频、拍照等方式对申请者的身份进行确认，也可以以面对面的方式进行确认。

4) GDCA may verify the information submitted by the subscriber through a voice communication, video, photo taking, etc. GDCA may also validate the information face to face.

5) 对于以某个组织中的个人身份名义申请的，还需要提交其所在单位提供的证明材料。

5) For the application applied by someone in his/her name who works in an organization, the applicant also needs to provide the proof materials from the organization, etc.

6) 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。如要求查询第三方数据库、发送确认电子邮件等。

6) When the application information contains some information of an organization, it is necessary to confirm the existence of the organization and whether the applicant belongs to the organization. GDCA could require validating by a third-party database, or sending e-mails to the organization, and so on.

如果认为有需要，GDCA 还可以通过从第三方获取的信息来验证该申请者个人的身份，如果 GDCA 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。

If necessary, GDCA can also verify the subscribers' identities using the information obtained from the third-party. If GDCA cannot get all the required information from a third-party, it may delegate the third-party to conduct an investigation or require certificate subscribers to provide additional information and evidence materials.

此外，必要时，GDCA 还可以设定其它所需要的鉴别方式和资料。

If necessary, GDCA may also establish other required identification methods and information.

申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。

The applicant is obliged to ensure the authenticity of the application materials and bear the corresponding legal responsibility.

对于 Adobe 个人文档签名证书，其身份鉴别方式遵循本节第 4 类个人证书的鉴别要求执行。

For Adobe Individual PDF signing certificates, GDCA follows the authentication requirements under Type IV Individual Certificate to perform identity validation.

3.2.3. 机构身份的鉴别 Authentication of Organization Identity

任何组织（政府机构、企事业单位等），在以组织名义申请机构类证书、设备类证书、SSL/TLS 服务器证书等各类型证书时，应进行严格的身份鉴别，包括如下内容：

Organizations (government agencies, enterprises and institutions, etc.), which apply for organization certificates, equipment certificates, SSL/TLS server certificates and other types of certificates, shall be authenticated strictly, including the following:

1. 确认机构是确实存在的、合法的实体。确认的方式可以是：政府机构签发的有效文件，包括但不限于工商营业执照或组织机构代码证等，或者通过签发有效文件的权威第三方数据库确认。

1. GDCA must authenticate the legal existence of the organization. Authentication attestation such as valid government issued documents, including but not limited to business license or organization

code certificate, or valid documents from authoritative third-party database.

2. 核查证书申请关键信息与有效文件或第三方数据库的资料是否相符，避免信息填写有误，但注册信息最终以申请者确认为准。

2. GDCA verifies to a reasonable level of assurance that key information in certificate application matches valid document or third-party database. But final confirmation of applicant's information shall govern.

3. 通过电话、邮政信函、被要求的证明文件或者与此类似的其它方式确认该组织资料信息的真实性，申请人是否得到足够的授权以及其它需要验证的信息。

3. GDCA shall verify the organization information through telephone, postal mail, required attestation or other similar methods.

4. 订户可采用面对面或者邮政信函等方式提交政府机构签发的有效文件。

4. Subscribers can submit valid government issued document through methods such as face-to-face submission or postal mail.

5. 确认经办人是否得到足够的授权，确认的方式可以是：组织机构授权给经办人申请办理证书事宜的授权文件及经办人有效身份证件的原件或者复印件。

5. GDCA authenticates the representative's authority to represent the applicant by checking authorized document from applicant and valid original and copy of personal ID.

GDCA 必须根据机构所申请的证书类别的不同，执行不同的身份鉴别方式，一般而言，证书类别越高，安全级别越高，鉴别方式越严格，鉴别内容越全面：

GDCA must perform different authentication methods depending upon the type of certificate applied by the organization. Generally, the higher class certificate type means higher security level, and stricter authentication method with more comprehensive authentication information.

1. 对于第 3 类机构证书，执行以下鉴别：

1. For the Type III Organization Certificate, the following authentication is performed:

1) 确认机构是确实存在的、合法的实体。确认的方式可以是：政府机构签发的有效文件，包括但不限于工商营业执照、企事业单位组织机构代码证等，或通过签发有效文件的权威第三方数据库确认。

1) Confirm the legal existence of organization. This can be proved by a valid document issued by a government agency, such as an Industrial and commercial business license, enterprise National Organization Code certificate, or validation through well-known authorized third-party database.

2) 确认授权申请的真实性，即代表组织机构提交证书申请的人是经过授权的。确认的方式可以是加盖公章的机构授权委托书及经办人有效身份证件文件或通过第三方得到的电话号码、邮政信函等方式与申请机构进行联络，以获得机构有关申请或授权事宜的确认。

2) GDCA must confirm the validity of the authorization, which means the agents who applied on behalf of organizations are authorized. Confirmation methods include checking organization authorization agreements with official seals, validating agents' valid ID, or contacting with the applicant by phone number or mailing address obtained from a third-party.

2. 对于第 4 类机构证书，执行以下鉴别：

2. For the Type IV Organization Certificate, the following authentication is performed:

1) GDCA 必须通过语音通话、视频、拍照等方式对申请机构提供的身份资料和申请材料进行确认，必要时应以面对面的方式进行确认。

1) GDCA must verify the identity and application information provided by the subscriber through voice communication, video, photo taking, etc. If necessary, GDCA may conduct a face-to-face confirmation.

2) 确认机构是确实存在的、合法的实体。确认的方式可以是：政府机构签发的有效文件，包括但不限于工商营业执照、企事业单位组织机构代码证等，并通过查询权威第三方数据库等方式对申请者及其申请材料进行验证，确保所提供的信息与核查结果一致。

2) Confirm the legal existence of organization. This can be proved by a valid document issued by a government agency, such as an Industrial and commercial business license, enterprise National Organization Code certificate, or validation through well-known authorized third-party database.

确认授权申请的真实性，即代表组织机构提交证书申请的人是经过授权的。确认的方式可以是加盖公章的机构授权委托书及经办人有效身份证件文件，并通过第三方得到的电话号码、邮政信函等方式与申请机构进行联络，以获得机构有关申请或授权事宜的确认。

Confirming the authenticity of the authorized application means that the person who submitted the certificate application on behalf of the organization is authorized. The confirmation method can be checking letter of attorney with organization's official seal and valid identity document of agent, contacting the applying organization via the phone number, postal mail and etc. from the third party to obtain confirmation about application or authorization of the applying organization.

此外，必要时，GDCA 还可以设定其它所需要的鉴别方式和资料。

If necessary, GDCA can also set other required identification methods and information.

对于 Adobe 机构文档签名证书，其身份鉴别方式遵循本节第 4 类机构证书的鉴别要求执行。

For Adobe Organization PDF signing certificates, GDCA follows the authentication requirements under Type IV Organization Certificate to perform identity validation.

3.2.4. 设备身份的鉴别 Authentication of Equipment Identity

设备身份的鉴别会根据其设备拥有者的不同而不同，GDCA 必须对订户进行身份鉴证，

包括如下内容：

Authentication on equipment identity varies by different according to different owners. GDCA must authenticate the identity of subscriber, including the following:

设备类订户需要提交数字证书申请表，设备拥有者身份证明的文件和复印件、业务办理授权书、经办人有效身份证件的原件和复印件。

Subscriber submits application form of equipment certificate with original and copy of owner's ID, authorization of operation, original and copy of delegated person's ID.

设备拥有者的身份鉴别根据不同类型按照不同的身份鉴别方式执行，订户为个人的，身份鉴别按照本 CP 第 3.2.2 节第 4 类个人证书鉴别流程执行；订户为机构的，按照本 CP 第 3.2.3 节第 4 类机构证书鉴别流程执行。

Authentication of Individual equipment Identity will be different according to the different owner of the equipment. If Subscriber are individuals, GDCA performs the verification of identity according to the CP section 3.2.2 class 4 personal certificate identification process; Subscriber are institutions, GDCA performs the verification of identity in accordance with the CP section 3.2.3 class 4 institutions certificate identification process.

在设备名称被作为证书主题内容申请证书时，还需要验证该申请者是否拥有该权利，确认的方式可以是提供归属权证明文件或机构对该设备所有权或使用权的书面承诺等，并加盖公章。

When the device name is applying for a certificate as the certificate subject content, GDCA also need to verify whether the applicants have the right to do so. Confirmation can be done as follows: Applicants shall provide the certificate of ownership or the written commitment of the ownership or use-right from the institution with company chop.

如果认为有需要，GDCA 还可以通过从第三方获取的信息来验证该申请者个人的身份，如果 GDCA 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。

If necessary, GDCA can also verify the applicants' identities using the information obtained from the third-party. If GDCA cannot get all the required information from a third-party, it may delegate a third-party to conduct an investigation or require certificate applicants to provide additional information and evidence material.

此外，必要时，GDCA 还可以设定其它所需要的鉴别方式和资料。

GDCA can also set other required identification methods and information.

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

GDCA 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：

（1）GDCA 向该邮件地址发送随机值，随机值由系统产生，并且唯一。

（2）申请者收到邮件并回复该随机值进行确认。

（3）GDCA 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。

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。鉴别方式遵循 S/MIME Baseline Requirements 1.0.0 第 3.2.2.2 节。

此外，对于含有个人身份信息的安全邮件证书，GDCA 将按照第 3.2.2 节第 4 类个人证书鉴别流程执行订户个人身份的鉴别；对于含有机构身份信息的安全邮件证书，GDCA 将按照 3.2.3 节第 4 类机构证书鉴别流程执行订户机构身份的鉴别。

GDCA or its authorized Registration Authorities will validate the validity and control of the e-mail address of the applicant by following procedures:

(1) GDCA sends a Random Value to the e-mail address; the Random Value will be generated by a system to ensure its uniqueness;

(2) The applicant receives the Random Value via an e-mail and sends back a confirming response with such Random Value;

(3) GDCA receives the Random Value from the applicant and compare such value with the one sent by GDCA, the validation completes once GDCA confirms that the Random Value received matches the one it sends.

The Random Value remains valid for use in a confirming response for no more than 24 hours from its creation. This way of validation conforms to section 3.2.2.2 of the S/MIME Baseline Requirements 1.0.0.

Additionally, for the S/MIME certificates that contain information of an individual, GDCA follows the authentication requirements for Type IV Individual Certificate as described in section 3.2.2 of this CP to perform identity validation for the individual. And for the S/MIME certificates that contain information of an organization, GDCA follows the authentication requirements for Type IV Organization Certificate as described in section 3.2.3 of this CP to perform identity validation for the organization.

3.2.6. SSL 服务器身份的鉴别 Authentication of SSL Server Identity

根据所签发的证书类型的不同执行不同的鉴别方式，包括如下内容：

GDCA must perform different authentication methods depending upon the types of SSL certificate applied by the subscribers.

对于 OV SSL 证书，需验证网站所有者机构的真实身份，其鉴别方式按照本 CP 第 3.2.3 节第 4 类机构证书鉴别流程执行。

For OV SSL certificate, GDCA shall validate the identity of the owner of website in accordance with the

Type IV organization authentication procedures in section 3.2.3 of CP.

对于 IV SSL 证书，需验证网站经营者个人真实身份，其鉴别方式按照本 CP 第 3.2.2 节第 4 类个人证书鉴别流程执行。

For IV SSL certificate, GDCA shall validate the identity of the owner of website in accordance with the Type IV individual authentication procedures in section 3.2.2 of CP.

对于 DV SSL 证书，只需验证个人或机构对网站域名的所有权或使用权，无需对机构或个人的真实身份进行验证。

For DV SSL certificate, GDCA shall validate the ownership or control of the domain name and will not verify the identity.

对于 EV SSL 证书，其鉴别方式遵循《GDCA EV 证书策略》，本 CP 不再对其进行具体阐述。

The validation procedures of EV SSL certificates is described in the GDCA EV CP and not covered in this document.

在域名被作为证书主题内容申请证书时，还需要验证该组织是否拥有该权利，对域名的鉴别按照本 CP 第 3.2.9 节执行。

In case of domain name is used as subject of certificate, GDCA shall validate whether the organization has the right and the validation of domain name is supposed to be in accordance with the CP section 3.2.9.

GDCA 不签发含有内部名称的 SSL 证书。

如果认为有需要，GDCA 还可以通过从第三方获取的信息来验证该申请者个人的身份，如果 GDCA 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。

GDCA does not issue SSL certificates containing internal names.

If necessary, GDCA can also verify the subscribers' identities using the information obtained from the third-party. If GDCA cannot get all the required information from a third-party, it may delegate the third-party to conduct an investigation or require certificate subscribers to provide additional information and evidence materials.

此外，必要时，GDCA 还可以设定其它所需要的鉴别方式和资料。

If necessary, GDCA may also establish other required identification methods and information.

3.2.7. 代码签名身份的鉴别 Authentication of CodeSigning Identity

普通代码签名身份的鉴别根据其代码拥有者的不同执行不同的身份鉴别方式，订户为机构的，按照本 CP 第 3.2.3 节第 4 类机构证书鉴别流程执行；订户为个人的，按照本 CP 第 3.2.2

节第 4 类个人证书鉴别流程执行。EV 代码签名身份的鉴别遵循《GDCA EV 证书策略》，本 CP 不再对其进行具体阐述。

Different authentication of subscribers' identity for a code signing certificate is performed based on different subscribers. For organization subscriber, GDCA performs certificate validation process in accordance with the Type IV organization authentication in CP section 3.2.3; for individual subscriber, GDCA performs certificate validation process in accordance with the Type IV individual authentication in CP section 3.2.2. The validation procedures of EV CodeSigning certificates is described in the GDCA EV CP and not covered in this document.

申请代码签名的订户，不论机构或个人，必须对其代码签名证书使用范围做出声明并提供证明文件，承诺不得将其代码签名证书用于对恶意软件、病毒代码、侵权软件、黑客软件等的签名。

Subscriber must make a statement and prove for the use of the CodeSigning certificate. Subscriber must promise not to sign malicious software, virus codes, infringement software and hacker software using the CodeSigning certificate.

3.2.8. 时间戳身份的鉴别 Authentication of TimeStamp Identity

GDCA 一般只针对机构签发时间戳证书。机构申请时间戳证书时，GDCA 需按照本 CP 3.2.3 节第 4 类机构证书鉴别流程执行。

GDCA generally issues Timestamp certificates only to organizations. For organizations that apply for Timestamp certificates, GDCA validates the identity of the organizations in accordance with the Type IV organization authentication procedures in section 3.2.3 of this CP.

3.2.9. 域名的确认和鉴别 Domain name recognition and Validation

对于域名的验证，被验证的实体还可以是申请者的母公司，子公司或附属机构，GDCA 可采用以下鉴别方式中的一种：

1. 通过该域名注册服务机构或权威第三方数据库中查询到的该域名持有者登记的电子邮件，通过邮件的方式发送随机值，验证方法为：（1）GDCA 向该邮件地址发送随机值，随机值由系统产生，并且唯一；（2）申请者收到邮件并回复该随机值进行确认；（3） GDCA 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，则鉴别通过。随机值的有效期最大为产生该随机值开始的 30 天。鉴别方式遵循 Baseline Requirements 2.1.7 第 3.2.2.4.2 节。【自 2024 年 12 月 27 日起，GDCA 不得依赖此方法进行域名验证。使用此方法进行的先前验证以及根据此方法收集的验证数据不得用于签发用户证书。】
2. 向域名联系人发送构建邮件，通过将一封包含随机值的邮件发送给由‘admin’，

‘administrator’，‘webmaster’，‘hostmaster’或‘postmaster’作为前缀加上符号@，以授权域名为尾缀的邮箱，并收到使用该随机值的确认回复（随机值的确认方法及有效期同上述第 1 种鉴别方式），确认其对域名的所有权或控制权。鉴别方式遵循 Baseline Requirements 2.1.7 第 3.2.2.4.4 节。

3. 通过确认申请域名在 DNS CNAME、TXT 或 CAA 记录中的任意值或请求令牌的存在来确认申请人对 FQDN（完全限定域名）的控制。鉴别方式遵循 Baseline Requirements 2.1.7 第 3.2.2.4.7 节。GDCA 按照本 CP 第 3.2.17 节的规定实施多视角签发验证（MPIC）。为了计入验证结果，网络视角必须监测到与主网络视角相同的挑战信息（即随机值或请求令牌）。
4. 通过确认请求值或随机值出现于某个文件的内容中（例如，某个请求值或随机值不出现于用于收取该文件的请求中，并收从请求中收到成功的 HTTP 2xx 状态代码回复），以确认申请者对 FQDN 的实际控制权。该鉴别方式遵循 Baseline Requirements 2.1.7 第 3.2.2.4.18 节。GDCA 按照本 CP 第 3.2.17 节的规定实施多视角签发验证（MPIC）。为了计入验证结果，网络视角必须监测到与主网络视角相同的挑战信息（即随机值或请求令牌）。

For the purpose of domain name validation, entities to be validated may also be the applicant's parent company, subsidiary company, or affiliate. GDCA may use one of the following ways for the validation of domain names:

1. Obtain the e-mail address of the domain name owner listed by the domain name registrar or other authoritative third party database, and contact the owner by sending a Random Value via email, and the validation steps include: (1) GDCA sends a Random Value to such e-mail address and the Random Value will be generated by a system to ensure its uniqueness; (2) The applicant receives the Random Value via an e-mail and sends back a confirming response with such Random Value; (3) GDCA receives the Random Value from the applicant and compare such value with the one sent by GDCA, the validation completes once GDCA confirms that the Random Value received matches the one it sends. The Random Value remains valid for use in a confirming response for no more than 30 days from its creation. This way of validation conforms to section 3.2.2.4.2 of the Baseline Requirements 2.1.7. [Effective December 27, 2024, GDCA shall not rely on this method for domain validation. Prior validations using this method and validation data gathered according to this method shall not be used to issue subscriber certificates.]
2. Sending an constructed email to domain contact to confirm the ownership and control of the domain name, by sending an email including a Random Value to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an authorized Domain Name, and receiving a confirming response utilizing the Random Value (GDCA follows the same steps to confirm a Random Value as described in 3.2.9.1). This way of validation conforms to section 3.2.2.4.4 of the Baseline Requirements 2.1.7.
3. By confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA

record to confirm the applicant's practical control over the FQDN. This way of validation conforms to section 3.2.2.4.7 of the Baseline Requirements 2.1.7. GDCA implements Multi-Perspective Issuance Corroboration as specified in section 3.2.17 of this CP. To count as corroborating, a network perspective must observe the same challenge information (i.e. Random Value or Request Token) as the primary network perspective.

4. Confirming the applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file (such as a Request Token, Random Number that does not appear in the request used to retrieve the file and receipt of a successful HTTP 2xx status code response from the request). This way of validation conforms to section 3.2.2.4.18 of the Baseline Requirements 2.1.7. GDCA implements Multi-Perspective Issuance Corroboration as specified in section 3.2.17 of this CP. To count as corroborating, a network perspective must observe the same challenge information (i.e. Random Value or Request Token) as the primary network perspective.

对于通配符域名，GDCA 验证通配符右侧的域名，保证该域名是明确归属于某一个商业实体、社会组织或政府机构等机构，并经过注册获得的。

GDCA 拒绝通配符（*）右侧的域名直接是顶级域名、公共后缀或由域名注册管理机构控制的域名的证书申请，除非申请者能够证明其完全控制该域名的所有命名空间。

必要时，GDCA 还需要采取其它独立的审查措施，以确认该域名的归属权，如果要求申请者提供相应的协助，该申请者不得拒绝这种请求。

As for the validation of a wildcard domain name, GDCA verifies the domain name in the right position of the wildcard to ensure the domain name in the right position of (*) is obtained through registration, and explicitly owned or controlled by a business entity, a social organization, or a government authority etc.

GDCA rejects any certificate request with a domain name in the right position of the wildcard (*) being a gTLD, public suffix, or a registry-controlled domain name, unless the applicant proves its rightful control of the entire domain namespace.

If necessary, GDCA may also perform the independent investigation to confirm the ownership of the domain name. The subscriber shall not refuse the requirements when corresponding assistance is needed from GDCA.

自 2026 年 3 月 15 日起，从主网络视角执行的所有与域名授权或控制权验证相关的 DNS 查询，GDCA 必须执基于 IANA DNSSEC 根信任锚的 DNSSEC 验证。用于主网络视角下所有域名授权或控制权验证相关 DNS 查询的 DNS 解析器必须：

- 按照 RFC 4035 第 5 节中定义的算法执行 DNSSEC 验证；
- 支持 RFC 5155 中定义的 NSEC3；
- 支持 RFC 4509 和 RFC 5702 中定义的 SHA-2；
- 正确处理 RFC 6840 第 4 节中列举的安全问题。

自 2026 年 3 月 15 日起，GDCA 不得使用本地策略禁用任何与域名授权或控制权验证相关的 DNS 查询的 DNSSEC 验证。

作为多视角签发验证的一部分，远程网络视角可以对与域名授权或控制权验证相关的 DNS 查询执行基于 IANA DNSSEC 根信任锚的 DNSSEC 验证。

基于 IANA DNSSEC 根信任锚的 DNSSEC 验证不在本 CP 第 8.7 节中的自评估范围内。

Effective March 15, 2026: DNSSEC validation back to the IANA DNSSEC root trust anchor must be performed on all DNS queries associated with the validation of domain authorization or control by the primary network perspective. The DNS resolver used for all DNS queries associated with the validation of domain authorization or control by the primary network perspective must:

- perform DNSSEC validation using the algorithm defined in RFC 4035 Section 5; and
- support NSEC3 as defined in RFC 5155; and
- support SHA-2 as defined in RFC 4509 and RFC 5702; and
- properly handle the security concerns enumerated in RFC 6840 Section 4.

Effective March 15, 2026: GDCA must not use local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control.

DNSSEC validation back to the IANA DNSSEC root trust anchor may be performed on all DNS queries associated with the validation of domain authorization or control by remote network perspectives used for Multi-Perspective Issuance Corroboration.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in section 8.7 of this CP.

3.2.10. 机构商业名称验证 Verification of DBA/Tradename

若证书主题中包含 DBA 或商业名称，GDCA 可通过以下方式中的至少一种以核实申请者有权使用该 DBA 或商业名称：

1. 申请者所在辖区的政府机构提供的可证明申请者合法成立、存在或认可的文档，或与该政府机构沟通；
2. 可靠的数据来源；
3. 与负责管理此类 DBA 名称或商业名称的政府机构沟通；
4. 附带支持文件的证明函件；
5. 物业账单，银行对账单，信用卡对账单，政府签发的税单，或其他 GDCA 认为可靠的验证方式。

If the subject identity information is to include a DBA or tradename, GDCA verifies that the applicants have right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the applicant's legal creation, existence, or recognition;

2. A reliable data source;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An attestation letter accompanied by documentary support; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that GDCA determines to be reliable.

3.2.11. 所在国的确认与鉴别 Verification of Country

若证书主题项中包含国家选项，GDCA 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。

In case the “countryName” field is present in the subject, GDCA verifies the country associated with the subject though checking the IP address of the applicant or the IP address on the DNS record from an authoritative third party database, to ensure the IP address of the applicant is consistent with a country where the applicant is actually located.

3.2.12. IP 地址的确认和鉴别 Authentication of an IP Address

GDCA 采用以下方式，确认申请者拥有或实际控制该 IP 地址：

1. 在包含 IP 地址的 URI（统一资源标识符）的在线网页上对约定的信息进行改动，通过此方式以确认申请者对 IP 地址的实际控制权。鉴别方式遵循 Baseline Requirements 2.1.7 第 3.2.2.5.1 节。GDCA 按照本 CP 第 3.2.17 节的规定实施多视角签发验证（MPIC）。为了计入验证结果，网络视角必须监测到与主网络视角相同的挑战信息（即随机值或请求令牌）。GDCA 不可为 IP 地址签发 EV SSL 证书。

GDCA adopts the following way for the authentication, to confirm the applicant owns or practically controls the IP address:

1. By making a change to the agreed-upon information found on an online Web page identified by a uniform resource identifier containing the IP address, to confirm the applicant’s practical control over the IP address. This way of validation conforms to section 3.2.2.5.1 of the Baseline Requirements 2.1.7. GDCA implements Multi-Perspective Issuance Corroboration as specified in section 3.2.17 of this CP. To count as corroborating, a network perspective must observe the same challenge information (i.e. Random Value or Request Token) as the primary network perspective.

GDCA must not issue EV SSL certificate for an IP address.

3.2.13. 数据来源的准确性 Data Source Accuracy

在将任何数据来源作为可依赖数据来源使用之前，GDCA 对该来源的可依赖性，准确性，及更改或伪造可抗性进行评估，并考虑以下因素：

1. 所提供信息的年限；
2. 信息来源更新的频率；
3. 数据供应商，及数据搜集的目的；
4. 数据对公众的可用性及可访问性；
5. 伪造或更改数据的相对难度。

对于 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 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不超过证书最大有效期，则 GDCA 可使用该数据及文件；对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 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不超过证书签发前 825 天，则 GDCA 可使用该数据及文件，对于根据本 CP 3.2.9（第 1 种验证方式除外）的要求获得的域名和 IP 地址，重用验证数据或文件的时间不超过证书签发前 398 天。

Prior to using any data source as a reliable data source, GDCA evaluates the source for its reliability, accuracy, and resistance to alteration or falsification, and considers the following during its evaluation:

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

GDCA may use the documents and data to verify certificate information, provided that it obtained the data or document no more than thirteen months prior to issuing the certificate.

For the subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, GDCA may use the documents and data to verify certificate information, provided that it obtained such data or document for a period no more than the maximum validity of the certificates. For the subscriber certificates issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT, 数安时代 R5 根 CA 证书, and GDCA TrustAUTH E5 ROOT, GDCA may use the documents and data to verify certificate information, provided that it obtained the data or document no more than 825 days prior to issuing the certificate, and for validation of domain names and IP addresses according to Section 3.2.9 (excluding validation method 1) of this CP, any reused data or document must be obtained no more than 398 days prior to issuing the certificate.

2020 年 10 月 1 日起，在使用某个实体登记/注册机构以满足 EV SSL 证书有关审核验证要求之前，GDCA 确保必须通过本 CP 章节 2.1 中所述的 GDCA 信息库，公开披露 EV SSL 证书审核验证所使用的实体登记/注册机构数据来源。其他类型的证书遵循该数据来源来进行机构身份的审核验证。

实体登记/注册机构的信息必须至少涵盖以下内容：

- 足够的信息以明确地识别实体登记/注册机构（例如名称、辖区及网站）；及
- 以下各项可接受的值：“subject:jurisdictionLocalityName”（OID: 1.3.6.1.4.1.311.60.2.1.1），“subject:jurisdictionStateOrProvinceName”（OID: 1.3.6.1.4.1.311.60.2.1.2），及“subject:jursidictionCountryName”（OID: 1.3.6.1.4.1.311.60.2.1.3），当使用实体登记/注册机构中的信息签发证书时，明示实体登记/注册机构适用的辖区；
- 当限制实体登记/注册机构使用的注册编号的格式或语法时，则需涵盖注册编号可接受的格式或语法；
- 修订记录，该清单的内容增加、修改及/或删除，则需涵盖唯一版本号及公开日期。

Effective as of 1 October 2020, GDCA shall ensure that, prior to the use of an Incorporating Agency or Registration Agency to fulfill the verification requirements for EV SSL certificates, the Incorporating Agency or Registration Agency data sources used for EV SSL Certificates will be publicly disclosed in the repository described in section 2.1 of this CP. GDCA also uses this data sources to validate the identities of organizations for other types of certificates.

This Agency Information shall include at least the following:

- Sufficient information to unambiguously identify the Incorporating Agency or Registration Agency (such as a name, jurisdiction, and website); and,
- The accepted value or values for each of the ‘subject:jurisdictionLocalityName’ (OID: 1.3.6.1.4.1.311.60.2.1.1), ‘subject:jurisdictionStateOrProvinceName’ (OID: 1.3.6.1.4.1.311.60.2.1.2), and ‘subject:jursidictionCountryName’ (OID: 1.3.6.1.4.1.311.60.2.1.3) fields, when a certificate is issued using information from that Incorporating Agency or Registration Agency, indicating the jurisdiction(s) that the Agency is appropriate for; and,
- The acceptable form or syntax of Registration Numbers used by the Incorporating Agency or Registration Agency, if the CA restricts such Numbers to an acceptable form or syntax; and,
- A revision history that includes a unique version number and date of publication for any additions, modifications, and/or removals from this list.

3.2.14. 没有验证的订户信息 Non-Verified Subscriber Information

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。

The information contained in the certificate must be validated, the information that is not validated shall

not be written into the certificate.

3.2.15. 授权确认 Validation of Authority

当机构订户授权经办人办理证书业务时，GDCA 应进行如下验证：

1. 通过第三方身份证明服务或数据库、政府主管部门签发的文件等方式确认该机构存在；
2. 通过机构授权文件、电话、有回执的邮政信函、雇佣证明或任何同等方式来验证该人属于上述机构以及其代表行为被该机构授权。

GDCA 应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 GDCA 不得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，GDCA 应向申请者提供其已授权人员的清单。

The following verification will be conducted while the representative of organization subscriber applying for certificate:

1. Confirming the organization from third-party identity verification service or database, documents issued by government.
2. Using telephone, postal letter with return receipt, employment proof document or any equivalent way to confirm that the person belongs to above organization and his/her behavior is authorized by these organization.

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

3.2.16. 互操作准则 Criteria for Interoperation

对于其他的电子认证服务机构，可以与 GDCA 进行互操作，但是该电子认证服务机构的 CPS 必须符合 GDCA CP 要求，并且与 GDCA 签署相应的协议。

Other certificate authorities can interoperate with GDCA. These CAs must ensure that their CPS are in compliance with the requirements from GDCA's CP and sign related agreement with GDCA.

GDCA 将依据协议的内容，接受非 GDCA 的发证机构鉴别过的信息，并为之签发相应的证书。

GDCA accepts the information authenticated by other CAs and issue corresponding certificates based on the agreement.

如果国家法律法规对此有规定，GDCA 将严格予以执行。

If there are provisions of national laws and regulations regarding interoperations of issuing certificate, GDCA will perform strictly according to relevant legislations.

截至目前，GDCA 未签发任何交叉证书。

To date, GDCA has not issued any cross certificates.

3.2.17. 多视角签发验证 Multi-Perspective Issuance Corroboration

多视角签发验证旨在在证书签发之前，通过来自多个远程网络视角的验证结果，对主网络视角所作出的判定（例如，域名验证通过/失败、CAA 许可/禁止）进行佐证。该过程有助于增强对等前缀的边界网关协议（BGP）攻击或劫持的防护能力。

GDCA 遵循 Baseline Requirements 的规则要求执行多视角签发验证。

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

GDCA follows the Baseline Requirements to perform multi-perspective issuance corroboration.

3.3. 密钥更新请求的标识与鉴别

Identification and Authentication for Re-key Requests

在进行 CP 第 4.7 节所述的证书密钥更新前，需对更新的密钥进行鉴别以确保密钥更新请求来自原证书密钥拥有者。

Before rekey operation described in CP section 4.7, GDCA shall authenticate the key to confirm that the request of rekey is from the original key owner.

3.3.1. 常规密钥更新的标识与鉴别

Identification and Authentication for Routine Re-key

对于常规情况下的密钥更新，订户可访问 GDCA 证书服务网站进行密钥更新申请，系统自动获取订户原证书信息，如甄别名、证书序列号等，形成证书密钥更新申请；GDCA 的证书认证系统将对密钥更新申请进行身份验证。订户也可以到GDCA的注册机构申请密钥更新，GDCA 注册机构必须验证订户与经办人的有效文件。

In general, subscriber can apply for rekey via GDCA certificate service website. The system can get former certificate information automatically such as DN, serial number, etc. Above operations can complete the application of rekey; Certificate authentication system of GDCA authenticates identity for rekey application. Subscriber can also apply for rekey to RA. RA must authenticate valid documents of subscriber and agent.

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，因此，订户在申请密钥更新前，必须确认使用原密钥对加密的文件或者数据已经解密，由此造成的损失，GDCA 将不承担责任。

The renewal of the secret key will cause that the original secret key is unable to decrypt the files or data. Therefore, the subscriber shall make sure the encrypted documents or data have been decrypted before they apply for the secret key's updating. GDCA shall not assume any responsibility due to failure of decryption by the renewal of the secret key.

对于第 1 类个人证书、第 2 类个人证书、设备类证书、服务器类证书、代码签名证书 GDCA 不接受密钥更新。

For Type I individual certificate, Type II individual certificate, equipment certificate, server certificates, and code signing certificate, GDCA does not accept key updates.

3.3.2. 撤销后密钥更新的标识与鉴别

Identification and Authentication for Re-key After Revocation

证书撤销后不能进行密钥更新。

Re-key/renewal after revocation is not permitted.

3.4. 撤销请求的标识与鉴别

Identification and Authentication for Revocation Request

证书撤销请求可以来自订户，也可以来自 GDCA、注册机构。当 GDCA 或者注册机构有本 CP4.9.1.1 所述理由撤销订户的证书时，有权依法撤销证书，这种情况无须进行鉴证。GDCA 或者注册机构的证书撤销请求，必须经过其管理机构或者监督机构进行确定才可以进行。如果订户主动请求撤销证书，则按照本 CP 第 3.2 节所述进行身份鉴别。如果是司法机关依法提出撤销，CA 或者 RA 将直接以司法机关书面的撤销请求文件作为鉴别依据，不再进行其他方式的鉴别。

Revocation requests can be made by subscriber, GDCA or RA. GDCA or RA can revoke certificate based on the reasons stated in section 4.9.1.1 of this CP without authentication. Revocation requests of GDCA or RA must be approved by its management or supervision authority. Subscribers who request to revoke certificates shall follow identity procedures described in CP section 3.2. If the revocation requests are from judicial authority by law, CA or RA will use revocation request documents of judicial authority as authentication evidence and will not use any other methods for authentication.

3.5. 授权服务机构的标识和鉴别 Identification and Authentication for Authorized Service Organization

适用于 GDCA ROOTCA 证书（RSA）、GDCA ROOT CA 证书、ROOTCA 证书（SM2）、GDCA ROOT CA1 证书签发的中级 CA 所签发的订户证书，RA 除了 GDCA 本身以外，GDCA 还可以授权 RA。

For subscriber certificates issued by the subordinate CAs which are issued by GDCA ROOTCA 证书（RSA）、GDCA ROOT CA 证书、ROOTCA 证书（SM2）、GDCA ROOT CA1, GDCA will serve as RA by itself, and may also assign another authorized RA.

对于授权的 RA，须有专门的安全运营场地，能有效防止、及时发现对运营场地的非授权进入。有专门的人员分别承担认证服务、系统运行维护和安全管理的职能。

The authorized RA must have a designated and secure operation location that can effectively prevent and detect unauthorized access; in addition, it must have designated personnel to undertake the functions in relation to certification services, system operation and maintenance, and security management.

授权 RA 应制定与 GDCA 一致的安全策略及运营管理规范，包括服务流程和规范、系统运行维护流程与规范，人员管理规范等，并经由 GDCA 确认后方可实施。

The authorized RA should formulate the security policies and operation management guidelines that are consistent with those adopted by GDCA, including service procedures and guidelines, system operation maintenance procedures, personnel management guidelines etc., which shall be implemented after confirmed and approved by GDCA.

GDCA 与授权 RA 签订相应的合作协议，授权 RA 须严格按本 CP $3.2 的要求执行身份鉴别。承担 RA 职责的人员须满足本 CP $5.3.1 的要求。同时授权 RA 应根据本 CP $ 5.5.2 的要求对文档和记录进行归档保存。

An agreement between GDCA and the authorized RA should be reached, under which the authorized RA shall perform identity authentication strictly according to section 3.2 of this CP. Relevant personnel undertaking the RA duties must meet the requirements of section 5.3.1 of this CP. In the meantime, the authorized RA must archive relevant documentation and records as required by section 5.5.2 of this CP.

GDCA 对授权 RA 的认证业务活动进行监控，检查其是否严格按照 GDCA 的安全策略及运营管理规范开展业务活动。如发现有违反策略、规范的情况，及时通知授权 RA 限期改正；若逾期不改，则 GDCA 立即暂停或终止授权 RA 的业务。

GDCA will monitor the certification services provided by the authorized RA to inspect whether or not its business activities comply with the security policies and operation management guideline adopted by GDCA. In case any violation of policies or guideline identified, GDCA will notify the authorized RA to take remediation actions within a given period, should no such actions taken within the given period, GDCA will suspend or terminate the business of the authorized RA immediately.

适用于 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的订户证书，GDCA 自行担任证书 RA，不再另行设立 RA。

For subscriber certificates issued by the subordinate CAs which are issued by GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA certificate and GDCA TrustAUTH E5 ROOT certificate, GDCA will serve as RA by itself, rather than assign another RA.

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(包括行政机关、事业单位、社会团体和人民团体等)。

Entities of certificate applicants may be individuals and organizations with independent legal entities (such as administrative organizations, institutions, social organizations, people's organizations and other organizations).

4.1.2. 注册过程与责任 Enrollment Process and Responsibilities

1. 注册过程

1. Registration Process

申请者将证书请求发送到 RA，RA 验证该请求，并对其签名，然后将其发送给 CA。

Applicant sends certificate request to RA. RA verifies and signs the request, then sends the results to CA.

CA 接收到该请求后，验证 RA 的签名，签发订户证书。在整个注册过程中，必须采取措施保证：

CA validates the RA signature after receiving the request and issues the end-user subscriber certificate. In the whole registration process, it is necessary to take enough measures to ensure that:

- RA 必须对申请信息和申请者的资料进行鉴别
- RA must verify the information of application and the identity of applicant.
- 在 RA 向 CA 发送证书请求时，保证传输信息过程安全、保密、完整
- RA ensures the security, confidentiality and integrity of information transmission in the process of sending certificate request to CA.

2. 责任

2. Responsibilities

- GDCA 及注册机构有责任向订户告知数字证书和电子签名的使用条件；
- GDCA and Registration Authority have the responsibility to inform the subscribers about the usage

condition of digital certificate and electronic signature.

- GDCA 及注册机构有责任向订户告知服务收费的项目和标准；

- GDCA and Registration Authority have the responsibility to inform the subscriber on service charging items and standards.

- GDCA 及注册机构有责任向订户告知保存和使用订户信息的权限和责任；

- GDCA and Registration Authority have the responsibility to inform the subscribers on the rights and responsibilities of preserving and using subscriber information.

- GDCA 及注册机构有责任向订户告知 GDCA 的责任范围；

- GDCA and Registration Authority have the responsibility to inform the subscribers on the responsibility scope of GDCA.

- GDCA 及注册机构有责任向订户告知订户的责任范围；

- GDCA and Registration Authority have the responsibility to inform the subscribers on the responsibility scope of subscriber.

- 订户应事先了解订户协议、CP 及 CPS 等文件约定的事项，特别是其中关于证书适用范围、权利、义务和担保的相关内容；

- The applicants should learn about the agreed-upon matters stipulated in the subscriber agreement, the CP and CPS etc. in advance, particularly those in relation to certificate usage, rights, obligations and warranties.

- 订户负有在其证书申请中提供准确信息的责任；

- The subscriber has the responsibility to provide accurate application information and data to GDCA.

- 注册机构承担对订户提供的证书申请信息与身份证明材料的一致性检查工作，同时承担相应审核责任。

- RAs shall ensure the consistency between certificate application information and identification which subscribers provided and bear corresponding responsibilities of review.

4.2. 证书申请处理 Certificate Application Processing

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

当 GDCA、注册机构接受到订户的证书申请后，应按本 CP 第 3.2 节的要求，对订户进行身份识别与鉴别。

对于 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 所签发的订户证书，若 GDCA 根据 CP 3.2 指定来源获得的数据或证明文件的时间不超过证书最大有效期且该信息未发生变化，则 GDCA 可使用该数据或证明文件，

核实证书中的信息；对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的订户证书，若 GDCA 根据 CP 3.2 指定来源获得的数据或证明文件的时间不超过 825 天（获得的域名和 IP 地址的验证数据或文件的时间不超 398 天）且该信息未发生变化，则 GDCA 可使用该数据或证明文件，核实证书中的信息。

After GDCA and its registration agencies receive the subscriber's certificate application, they will perform identity recognition and verification of identification over the subscriber according to the requirements of CP section 3.2.

For the subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, GDCA may use the documents and data to verify certificate information, provided that it obtained the data or document (according to section 3.2 of this CP) for a period no more than the maximum validity of the certificates, and provided that no changes occurred to the documents and data within such time period. For the subscriber certificates issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT, 数安时代 R5 根 CA 证书, GDCA may use the documents and data to verify certificate information, provided that it obtained the data or document (according to section 3.2 of this CP) no more than 825 days prior to issuing the certificate (and for validation of domain names and IP addresses, any reused data or document must be obtained no more than 398 days prior to issuing the certificate), and provided that no changes occurred to the documents and data within such time period.

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

GDCA、注册机构应在鉴证的基础上，批准或拒绝申请。如果拒绝申请，则应该通过适当的方式、在合理的时间内通知证书申请者。

GDCA and RA should approve or reject applications based on authentication. If GDCA and RA reject an application, they should inform the applicants with appropriate ways and within reasonable time period.

4.2.2.1. 证书申请的批准 Approval of Certificate Applications

如果符合下述条件，RA 可以批准证书申请：

1. 该申请完全满足本 CP 第 3.2 节关于订户身份的标识和鉴别规定；
2. 申请者接受或者没有反对订户协议的内容和要求；
3. 申请者已经按照规定支付了相应的费用。

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

1. The application shall completely meet the requirements from CP section 3.2 regarding the subscriber's identification information and authentication.
2. Applicant accepts or has no opposition regarding the content or requirements of the subscriber's agreement.
3. Applicant has paid already in accordance with the provisions.

4.2.2.2. 证书申请的拒绝 Rejection of Certificate Applications

如果发生下列情形，RA 应拒绝证书申请：

RA shall refuse the certificate application in case of the following situations:

1. 该申请不符合本 CP 第 3.2 节关于订户身份的标识和鉴别规定；

1. The application does not meet the specifications of subscriber's identification and authentication in CP section 3.2.

2. 申请者不能提供所需要的身份证明材料；

2. The applicant can't provide the required identity documents.

3. 申请者反对或者不能接受订户协议的有关内容和要求；

3. The applicant opposes or cannot accept the relevant content or requirements of the subscriber's agreement.

4. 申请者没有或者不能够按照规定支付相应的费用；

4. The applicant has not paid or can't pay the appropriate fees.

5. 申请的证书含有 ICANN（The Internet Corporation for Assigned Names and Numbers）考虑中的新 gTLD（顶级域名）；

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

6. GDCA 或者注册机构认为批准该申请将会对 GDCA 带来争议、法律纠纷或者损失。

6. GDCA or RA considers that the approval of the application will bring about controversies, legal disputes or losses to the GDCA.

对于 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的订户证书，如果法律法规明确禁止某个申请，或 GDCA 认为批准该申请具有高风险性，GDCA 应拒绝该申请，GDCA 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，或 GDCA 之前由于怀疑网络钓鱼或其他诈骗用途或顾虑而拒绝的证书请求或撤销的证书，建立和维护证书高风险申请人列表，在接受证书申请时将会查询该列表信息。对于列表中出现的申请人，GDCA 将直接拒绝其申请。

对于拒绝的证书申请，GDCA 通知申请者证书申请失败。

For the subscriber certificates issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA 证书 and GDCA TrustAUTHE5 ROOT, if the application is prohibited clearly by laws and regulations, or GDCA considers that there are highly risks to approve the application, GDCA shall reject it. GDCA establishes and maintains a list of high risk certificate applicants according to the list provided by anti-phishing alliance, antivirus vendor or related alliance, government agencies which are

responsible for network security affairs and other third parties, or the disclosure of information through public media reports, or previously rejected certificate requests by GDCA due to suspected phishing or other fraudulent usage or concerns. GDCA will query information from the list during accepting certificate application. If the applicants appear in this list, GDCA will reject their application directly.

For the rejected certificate application request, GDCA will notify the applicant about the failure of application.

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

GDCA 的电子认证业务规则（CPS）应规定合理的证书申请处理时间。GDCA 和注册机构应在 CPS 规定的时间内处理证书申请，无论是批准还是拒绝。这个时间通常是 2 个工作日。

GDCA CPS should specify the processing period of certificate application. No matter approving or rejecting, GDCA and RA should process certificate application within the period specified by CPS. The period is 2 working days in general.

4.2.4. 认证机构授权（CAA） Certification Authority Authorization (CAA)

对于 GDCA 颁发的满足 CA/浏览器论坛 EV Guidelines、Baseline Requirements 要求的公共可信的 SSL/TLS 证书，GDCA 对签发证书主题别名扩展项中的每一个 dNSName 做 CAA 记录检查，并遵循查询到的指示。

GDCA 根据 RFC8659 的规定处理“issue”、“issuewild”及“iodef”的属性标签：若“issue”、“issuewild”标签中不包含“gdca.com.cn”，则 GDCA 不签发对应的证书；若 CAA 记录中出现“iodef”标签，则 GDCA 与申请者沟通后决定是否为其颁发证书。

GDCA 应以下列 CAA 记录查找失败情况作为可签发证书的条件：1）在非 GDCA 的基础设施中查询 CAA 记录失败；2）至少尝试过一次重新查找 CAA 记录；3）GDCA 已确认该域名属于 RFC 4035 第 4.3 节所定义的“不安全”状态。

For the publicly trusted SSL/TLS certificates issued by GDCA and conform to the EV Guidelines and Baseline Requirements of the CA/Browser Forum, GDCA will check the CAA records and follow the processing instructions found for each dNSName in the subjectAltName extension of the certificate to be issued.

GDCA shall process "issue", "issuewild", and “iodef” property tags according to RFC8659: GDCA shall not issue corresponding certificates if the "issue", "issuewild" property tags do not contain “gdca.com.cn”. In case the property tag “iodef” is present in the CAA records, GDCA shall determine whether or not to issue certificates after communicating with the applicant.

GDCA shall treat a record lookup failure as permission to issue certificates if: 1) the failure is outside the GDCA's infrastructure; 2) the lookup has been retried at least once; and 3) GDCA has confirmed that the domain is “Insecure” as defined in RFC 4035 Section 4.3.

4.2.4.1. CAA 记录的 DNSSEC 验证 DNSSEC Validation of CAA Records

自 2026 年 3 月 15 日起，从主网络视角执行的所有与 CAA 记录查询相关的 DNS 查询，GDCA 都必须执行基于 IANA DNSSEC 根信任锚的 DNSSEC 验证。用于主网络视角下所有 CAA 记录查询相关 DNS 查询的 DNS 解析器必须：

- 按照 RFC 4035 第 5 节中定义的算法执行 DNSSEC 验证；
- 支持 RFC 5155 中定义的 NSEC3；
- 支持 RFC 4509 和 RFC 5702 中定义的 SHA-2；
- 正确处理 RFC 6840 第 4 节中列举的安全问题。

自 2026 年 3 月 15 日起，GDCA 不得使用本地策略禁用任何与 CAA 记录查询相关的 DNS 查询的 DNSSEC 验证。

自 2026 年 3 月 15 日起，主网络视角在 DNSSEC 验证过程中发现的错误（例如 SERVFAIL）不得被视为证书签发的许可。

作为多视角签发验证的一部分，远程网络视角可以对与 CAA 记录查询相关的所有 DNS 查询执行基于 IANA DNSSEC 根信任锚的 DNSSEC 验证。

基于 IANA DNSSEC 根信任锚的 DNSSEC 验证不在本 CP 第 8.7 节中的自评估范围内。

Effective March 15, 2026: DNSSEC validation back to the IANA DNSSEC root trust anchor must be performed on all DNS queries associated with CAA record lookups performed by the primary network perspective. The DNS resolver used for all DNS queries associated with CAA record lookups performed by the primary network perspective must:

- perform DNSSEC validation using the algorithm defined in RFC 4035 Section 5; and
- support NSEC3 as defined in RFC 5155; and
- support SHA-2 as defined in RFC 4509 and RFC 5702; and
- properly handle the security concerns enumerated in RFC 6840 Section 4.

Effective March 15, 2026: GDCA must not use local policy to disable DNSSEC validation on any DNS query associated CAA record lookups.

Effective March 15, 2026: DNSSEC-validation errors observed by the primary network perspective (e.g., SERVFAIL) must not be treated as permission to issue.

DNSSEC validation back to the IANA DNSSEC root trust anchor may be performed on all DNS queries associated with CAA record lookups performed by remote network perspectives as part of Multi-Perspective Issuance Corroboration.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in section 8.7 of this CP.

4.3. 证书签发 Certificate Issuance

4.3.1. 证书签发中 RA 和 CA 的行为 CA Actions During Certificate Issuance

根 CA 的证书签发应由 GDCA 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。

A trusted person authorized by GDCA should deliberately issue a direct command with respect to certificate issuance by the root CA, in order for the root CA to perform a certificate signing operation.

在证书的签发过程中 RA 的管理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 发往 CA 的证书签发请求信息须有 RA 的身份鉴别与信息保密措施，并确保请求发到正确的 CA 证书签发系统。

In the process of issuing certificate, the RA's administrator is responsible for the approval of certificate application, and sending certificate issuance request to the certificate issuance system of CA via the RA system. Issuance request which RA sends to CA must include identification with the measures of information security. RA must ensure that the request is sent to the correct CA certificate issuance system.

CA 的证书签发系统在获得 RA 的证书签发请求后，对来自 RA 的信息进行鉴别与解密，对于有效的证书签发请求，证书签发系统签发订户证书。

After obtaining the RA certificate issuance request, CA certificate issuance system authenticates and decrypts the requests. For the valid certificate issuing request, certificate issues system issues the subscriber certificate.

对于 2025 年 3 月 15 日当天或之后签发的 SSL/TLS 证书，在证书签发之前，GDCA 必须对待签名证书（TBS 证书）进行 linting 检测。

For SSL/TLS certificates issued on or after March 15, 2025, GDCA must perform pre-issuance linting to check the tbsCertificate (to be signed Certificate).

4.3.2. CA 和 RA 通知订户证书的签发

Notifications to Subscriber by the CA of Issuance of Certificate

GDCA 的证书签发系统签发证书后，将直接或者通过 RA 通知订户证书已被签发，并向订户提供可以获得证书的方式，包括通过面对面、网络下载等方式，或者通过其它与订户约定的方式告知订户如何获得证书。

After GDCA certificate issuance system issues certificates, subscribers will be informed by GDCA or RA that the certificate is issued and how to obtain certificates. Subscriber can get the certificate via face-face, online download, or other methods specified by subscriber.

4.4. 证书接受 Certificate Acceptance

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

1. 订户自行访问专门的 GDCA 证书服务网站将证书下载至本地存放介质，如本地计算机、USB Key 中，证书下载完毕即代表订户接受了证书。

1. Subscribers access to specialized GDCA certificate service website, then download certificate to the certificate carrier, that means subscriber totally accepted the certificate after it has been downloaded.

2. GDCA 注册机构代替订户下载证书，下载的证书将被保存在数字证书载体中，当订户接受了该数字证书载体即代表订户接受了证书。

2. When RA of GDCA downloads the certificate on behalf of subscriber, the downloaded certificate will be kept in digital certificate carrier. Once the subscribers accept the certificate carrier, the subscribers accept the certificate.

3. 订户接受了获得证书的方式，并且没有提出反对证书或者证书中的内容。

3. Subscribers have received the way of obtaining the certificates, and no objection of the certificates or their contents.

4. 订户反对证书或者证书内容的操作失败。

4. Subscribers fail to oppose or conduct the operation of objection over the certificates or the content of certificates.

4.4.2. CA 对证书的发布 Publication of the Certificate by the CA

订户接受证书后，GDCA 将该订户证书发布到 GDCA 的目录服务系统。同时，GDCA 根据 Google 的 CT 策略（https://github.com/chromium/ct-policy），将订户的域名信息发布在至少三个 CT 服务器中。

After a subscriber receives a certificate, GDCA publishes the subscriber certificate to directory service system. As per the Google CT policy (https://github.com/chromium/ct-policy), GDCA embeds in the SSL/TLS certificates the signature data from at least three CT servers recognized by Google.

4.4.3. CA 通知其他实体证书的签发 Notification of Certificate Issuance by the CA to Other Entities

除证书订户外，GDCA 及注册机构不需要通知其他实体证书的签发。

GDCA and RA do not need to notify the certificate issuance to other entities except for subscribers.

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 GDCA 所签发的证书后，均视为已经同意遵守与 GDCA、依赖方有关的权利和义务的条款。订户接受到数字证书，应采取合理措施妥善保存其证书对应的私钥避免未经授权的使用。订户只能在适用的法律、本 CP 以及订户协议规定的范围内使用私钥和证书。

对于签名证书，其私钥可用于对信息的签名，订户应知悉并确认签名的内容。对于加密证书，其私钥可用于对采用对应公钥加密的信息进行解密。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。

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

After the subscribers have submitted certificate application and received certificates issued by GDCA, they are deemed to have agreed to comply with the terms of GDCA, relying party related rights and obligations. The subscriber who receives the certificate shall take appropriate measures to properly keep the corresponding private key to the certificate from unauthorized use. Subscribers can only use the private key and certificate in the CP specified range, and under applicable laws and the subscriber agreement.

For the signature certificate, the private key can be used for the signature of a message. The subscriber should know about and confirm the signature content. For the encryption certificate, the private key can be used to decrypt the information which uses the corresponding public key to encrypt. After the certificate expires or is revoked, the subscriber must stop using the certificate's corresponding private key.

For the SSL/TLS certificates, the subscribers should undertake an obligation and warranty to install the certificates only on servers that are accessible at the subjectAltName(s) listed in the certificates.

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

当依赖方接收到加载数字签名的信息后，有义务进行以下确认操作：

When the relying party has received the message with digital signature, the party has the obligation to carry out the following operations to confirm:

1. 获得数字签名对应的证书及信任链；

1. Obtain digital signature's corresponding certificate and trust chain.

2. 确认该签名对应的证书是由 GDCA 所签发；

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

3. 通过查询 CRL 或 OCSP 确认该签名对应的证书是否被撤销；

3. Confirm whether the signature corresponding certificate has been revoked by querying the CRL or OCSP.

4. 证书的用途适用于对应的签名；

4. Certificate usage is suitable for the corresponding signature.

5. 使用证书上的公钥验证签名。

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

6. 检查证书的有效期

6. Check the validity of the certificates

以上任何一个环节失败，依赖方有责任拒绝签名信息。

If the above conditions are not met, relying party has the responsibility to refuse to sign information.

当依赖方需要发送加密信息给接受方时，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密。依赖方应将加密证书连同加密信息一起发送给接受方。

When the relying party needs to send an encrypted message to the receiving party, the party must first obtain the encryption certificate of receiving party through proper channels, and then encrypt the information using public key of the certificate. The relying party should send the encryption certificate and encrypted information to receiving party.

4.6. 证书更新 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。

Certificate renewal is the issuance of a new certificate to the subscriber without changing the public key or any other information in the certificate.

4.6.1. 证书更新的情形 Circumstances for Certificate Renewal

对于 GDCA 签发给订户的证书，订户需在证书到期前进行证书更新。

对于由 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 所签发的订户证书，订户可访问 GDCA 证书服务网站或者到 GDCA 的注册机构进行证书更新的申请。申请证书更新无需填写注册信息，系统会自动获取所需的信息。

对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的订户证书，订户需按新申请的要求提交注册信息。证书过

期后，订户必须重新申请新证书。

对于 SSL/TLS 证书，GDCA 接受订户在不更新密钥时申请更新证书。订户申请更新证书时，GDCA 需对订户提交的密钥进行检查，以确认其是否为弱密钥，如为弱密钥，则要求订户提交符合要求的密钥。

For the subscriber certificates issued by GDCA, the subscribers need to submit the certificate update request before the expiry of the certificate.

For the subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, the subscriber can access the GDCA Certificate Services Website or GDCA Registration Authority for certificate renewal application before expiration. Applicant for certificate renewal has no need to fill in the registration information, while the system will automatically obtain the information.

For the subscriber certificates issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT, 数安时代 R5 根 CA 证书, and GDCA TrustAUTH E5 ROOT, when renewing the certificates, the subscribers shall submit the registration information as they do for the new certificates requests. If the certificate had expired, the subscriber must apply for a new certificate.

For SSL/TLS certificate, GDCA accepts the subscriber to apply for certificate renewal without updating the key. When a subscriber requests to renew a certificate, GDCA will check whether a key submitted is a weak key, and will require the subscriber to renew the key pair if the submitted key is proved to be weak.

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。

The entity who requests certificate update is the subscriber.

4.6.3. 处理证书更新请求 Processing Certificate Renewal Requests

对于证书更新，其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：

For certificate renewal, its process includes application and verification, identification, and issuance of the certificate. The verification and authentication of application shall be based on the following:

1. 订户的原证书存在并且由 GDCA 所签发；

1. The original certificate of subscriber is exist and issued by GDCA

2. 验证证书更新请求在许可期限内；

2. Validate the certificate update request is in validity period.

3. 基于原注册信息进行身份鉴别。

3. Identity verification based on the original registration information.

在以上验证和鉴别通过后 GDCA 才可批准签发证书。

GDCA can issue certificate only if all the verification and identification above are passed.

订户也可以选择一般的初始证书申请流程进行证书更新，按照要求提交相应的证书申请和身份证明资料。GDCA 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。

When the certificate is updated, subscribers can use the original private key to sign the update request, and GDCA will verify and identify the validity, legality and uniqueness of subscriber's signature and public key, user information of the update request.

4.6.4. 通知订户新证书的签发

Notification of New Certificate Issuance to Subscriber

同本 CP 第 4.3.2 节。

See CP section 4.3.2

4.6.5. 构成接受更新证书的行为

Conduct Constituting Acceptance of a Renewal Certificate

同本 CP 第 4.4.1 节。

See CP section 4.4.1

4.6.6. CA 对更新证书的发布

Publication of the Renewal Certificate by the CA

同本 CP 第 4.4.2 节。

See CP section 4.4.2

4.6.7. CA 通知其他实体证书的签发

Notification of Certificate Issuance by the CA to Other Entities

同本 CP 第 4.4.3 节。

See CP section 4.4.3

4.7. 证书密钥更新 Certificate Rekey

证书密钥更新指订户或其他参与者生成一对新密钥并申请为新公钥签发一个新证书。

Certificate Rekey refers to generating a new key and requesting to issue a new certificate for the new public key by the subscriber or other participants.

4.7.1. 证书密钥更新的情形 Circumstances for Certificate Rekey

GDCA 的证书密钥更新包括但不限于以下情形：

GDCA certificate Re-key including but not limited to the following circumstances:

1. 证书私钥泄露而撤销证书；

1. Revocation certificate due to private key leakage.

2. 证书到期；

2. The certificate expires.

3. 基于技术、政策安全原因，GDCA 要求证书密钥更新。

3. GDCA requires certificate key update based on the security reasons of technology and policy.

4.7.2. 请求证书密钥更新的实体

Who May Request Certification of a New Public Key

请求证书密钥更新的实体为证书订户。

The entity who requests re-key is the certificate subscriber.

4.7.3. 处理证书密钥更新请求 Processing Certificate Rekeying Requests

同本 CP 第 4.6.3 节。

See CP section 4.6.3.

4.7.4. 通知订户新证书的签发

Notification of New Certificate Issuance to Subscriber

同本 CP 第 4.3.2 节。

See CP section 4.3.2.

4.7.5. 构成接受密钥更新证书的行为

Conduct Constituting Acceptance of a Rekeyed Certificate

同本 CP 第 4.4.1 节。

See CP section 4.4.1.

4.7.6. CA 对密钥更新证书的发布

Publication of the Rekeyed Certificate by the CA

同本 CP 第 4.4.2 节。

See CP section 4.4.2.

密钥更新证书应在 24 小时内发布。

Re-Keyed Certificate must be published within 24 hours.

4.7.7. CA 通知其他实体证书的签发

Notification of Certificate Issuance by the CA to Other Entities

同本 CP 第 4.4.3 节。

See CP section 4.4.3.

4.8. 证书变更 Certificate Modification

4.8.1. 证书变更的情形 Circumstances for Certificate Modification

如果订户提供的注册信息发生改变，必须向 GDCA 提出证书变更。

If the registered information which subscriber provide is changed, the subscriber has the obligation to report certificate modification to the GDCA.

如果证书内包含信息的变更可能影响订户权利义务的改变，则订户不能申请证书变更，只能撤销该证书，再重新申请新的证书。

If information contained in the certificate changes that may affect the rights and obligations of subscribers. The subscriber cannot apply for the certificate change, and he/she can only revoke the certificate then apply for a new certificate again.

证书变更的申请和证书申请所需的流程、条件是一致的。

Both of the procedure and conditions of the certificate application and modification is the same.

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。

The entity who requests the certificate modification is the subscriber of the certificate.

4.8.3. 处理证书变更请求 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，同本 CP 3.2。

The certificate modification is processed following the registration procedures where the first application for a certificate, see CP 3.2.

4.8.4. 通知订户新证书的签发 Notification of New Certificate Issuance to Subscriber

同本 CP 第 4.3.2 节。

See CP section 4.3.2

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

同本 CP 第 4.4.1 节。

See CP section 4.4.1

4.8.6. CA 对变更证书的发布 Publication of the Modified Certificate by the CA

同本 CP 第 4.4.2 节。

See CP section 4.4.2

4.8.7. CA 通知其他实体证书的签发 Notification of Certificate Issuance by the CA to Other Entities

同本 CP 第 4.4.3 节。

See CP section 4.4.3

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. 订户证书撤销的原因 Reasons for Revoking a Subscriber Certificate

若出现以下情况中的一种或多种，GDCA 必须在 24 小时之内撤销证书：

1. 订户以书面形式请求撤销证书；
2. 订户通知 GDCA 最初的证书请求未得到授权且不能追溯到授权行为；
3. GDCA 获得了证据，证明与证书公钥对应订户私钥遭到了泄漏；
4. GDCA 获得了证据，证明对证书中 FQDN，IP 地址或邮箱地址的域名授权或控制权的验证不应被依赖；
5. CA 被告知出现了可使订户私钥泄露的经验证的方法，此类方法可根据公钥轻易地计算私钥值（例如 Debian 弱密钥，见：http://wiki.debian.org/SSLkeys），或存在明确的证据。

若出现以下情况中的一种或多种，CA 应在 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 Baseline Requirements 第 6.1.5 节及第 6.1.6 节；
2. GDCA 获得了证书遭到误用的证据；
3. GDCA 获悉订户违反了订户协议、CP/CPS 中的一项或多项重大责任；
4. GDCA 获悉了任何表明 FQDN 或 IP 地址的使用不再被法律许可（例如，某法院或仲裁员已经撤销了域名注册人使用域名的权力，域名注册人与申请人的相关许可及服务协议被终止，或域名注册人未成功更新域名）；
5. GDCA 获悉某通配符证书被用于鉴别具有欺骗误导性的子域名；
6. GDCA 获悉证书中所含信息出现重大变化；
7. GDCA 获悉证书的签发未能符合 Baseline Requirements 要求，或 GDCA 的 CP 或 CPS；
8. GDCA 认为任何或被告知出现在证书中的信息为错误信息；
9. GDCA 依据 Baseline Requirements 签发证书的权力失效，或被撤销或被终止，除非其继续维护 CRL/OCSP 信息库；
10. CPS 中职责的履行被延迟或受不可抗力的阻碍；自然灾害；计算机或通信失败；法律、规章或其它法律的改变；政府行为；或其它超过个人控制的原因并且对他人信息构成威胁的；

11. GDCA 已经履行催缴义务后，订户仍未缴纳服务费；

GDCA shall revoke a certificate within 24 hours if one or more of the following occurs:

1. The subscriber requests in writing that GDCA revoke the certificate;
2. The subscriber notifies GDCA that the original certificate request was not authorized and does not retroactively grant authorization;
3. GDCA obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise;
4. GDCA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name. IP address or mailbox address in the certificate should not be relied upon; or
5. GDCA is made aware of a demonstrated or proven method that exposes the subscriber's private key to compromise, methods have been developed that can easily calculate it based on the public key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).

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

1. The certificate no longer complies with the Baseline Requirements section 6.1.5 and 6.1.6;
2. GDCA obtains evidence that the certificate was misused;
3. GDCA is made aware that a subscriber has violated one or more of its material obligations under the subscriber agreement and CP/CPS;
4. GDCA 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. GDCA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name;
6. GDCA is made aware of a material change in the information contained in the certificate;
7. GDCA is made aware that the certificate was not issued in accordance with Baseline Requirements or GDCA’s CP or CPS;
8. GDCA determines or is made aware that any of the information appearing in the certificate is inaccurate;
9. GDCA’s right to issue certificates under the Baseline Requirements expires or is revoked or terminated, unless it has made arrangements to continue maintaining the CRL/OCSP repository;
10. The fulfillment of the obligations in the CPS is delayed or encounters force majeure, such as natural disasters, computer or communications failures, changes of laws and regulations, government actions or other causes beyond the reasonable control, causing threats to the information of others; or

11. Subscribers fail to pay the service fees after GDCA performed the obligations of notifying the subscribers to pay.

发生下列情形，对于 GDCA 证书服务系统中使用的证书，例如 CA、RA、受理点或其它服务主体（包括服务系统中的设备使用的证书）使用的证书，可以撤销其证书：

1. CA 与 RA、受理点等签订的协议终止或者发生改变；
2. 证书私钥发生安全性损害或者被怀疑发生安全性损害；
3. 出于管理的需要。

If the following circumstances occur, for the certificates using in GDCA certificate service system, such as certificate using in CA, RA, LRA or other services entities (including equipment using certificate in service system), GDCA can revoke the certificate:

1. Agreement between GDCA and RA, LRA has changed or stopped.
2. The private key of the certificate has security damage or is suspected with security damage.
3. The need of management.

证书订户如果发现或者怀疑证书私钥安全发生损害，应立即通知 CA 进行撤销。对于 SSL/TLS 服务器类证书，若出现以下任意一项或几项情形，也需进行证书撤销操作：

1. CA 机构得知域名不在合法，如被法院判定该域名非法、与域名注册机构的合约终止等；
2. CA 机构得知一个通配符证书被用来验证一个欺诈性的误导子域名；
3. CA 机构由于某种原因终止运行，并且未安排其他 CA 提供撤销证书的支持性操作；
4. CA 签发证书的权利已届满或被撤销或终止，除非 CA 已作出安排，继续维护 CRL/OCSP；
5. 证书的技术内容或格式造成了对应用软件供应商或依赖方不可接受的风险。

If certificate subscribers discover or suspect the security of private key of the certificate has been damaged, they shall immediately notify GDCA to revoke the certificate. For the SSL/TLS server certificate, if the following one or several cases have occurred, GDCA also need to carry out the certificate revocation:

1. Domain name that CA knows is no longer valid, such as the domain name has been judged by the court, domain name registration agency contract termination, etc.
2. GDCA knew a wildcard certificate was used for a fraudulent misrepresentation sub domain name.
3. GDCA terminates the operation for some reasons and doesn’t arrange other CA to provide for supporting operation of revocation certificates.
4. Unless GDCA make special arrangements, GDCA will continue to maintain CRL/OCSP, under the circumstance of that GDCA’s right to issue certificate has been expired, revoked or terminated.
5. Technical content or format of certificate causes unacceptable risk for application software vendor or relying party.

4.9.1.2. 中级 CA 证书的撤销原因 Reasons for Revoking a Subordinate CA Certificate

若出现以下情况中的一种或多种，GDCA 须在 7 天之内撤销中级 CA 证书：

1. GDCA 获得了证据，证明与证书公钥对应的中级 CA 私钥遭到了损害，或不再符合 Baseline Requirements 或 S/MIME Baseline Requirements 第 6.1.5 节及第 6.1.6 节的相关要求；
2. GDCA 获得了证书遭到误用的证据；
3. GDCA 获悉证书的签发未能符合 Baseline Requirements 要求，或中级 CA 未能符合 CP/CPS；
4. GDCA 认为任何出现在中级 CA 证书中的信息不准确、不真实或具有误导性；
5. GDCA 由于任何原因停止运营，且未与另一家 CA 达成协议以提供证书撤销服务；
6. GDCA 依据 Baseline Requirements 签发证书的权力失效，或被撤销或被终止，除非其继续维护 CRL/OCSP 信息库。

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

1. GDCA 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 Sections 6.1.5 and 6.1.6 of Baseline Requirements or S/MIME Baseline Requirements;
2. GDCA obtains evidence that the certificate was misused;
3. GDCA is made aware that the certificate was not issued in accordance with Baseline Requirements or that subordinate CA has not complied with the GDCA CP or CPS;
4. GDCA determines that any of the information appearing in the subordinate CA certificate is inaccurate, unreal or misleading;
5. GDCA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
6. GDCA's right to issue certificates under Baseline Requirements expires or is revoked or terminated, unless GDCA has made arrangements to continue maintaining the CRL/OCSP Repository.

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

以下实体可以请求撤销一个订户证书：

1. GDCA 或注册机构可以依据本 CP 第 4.9.1 节 要求撤销一个订户证书；
2. 对于个人证书，证书订户可以请求撤销他们自己的个人证书；
3. 对于机构证书，只有机构授权的代表有资格请求撤销已经签发给该机构的证书；
4. 对于设备证书，只有拥有设备的机构授权的代表有资格请求撤销已经签发的证书；
5. 法院、政府主管部门及其他公权力部门可以依法撤销订户证书。
6. 依赖方、应用软件提供商、防病毒机构或其他的第三方可以提交证书问题报告，告知

GDCA 有合理理由撤销证书。

The following entities can request revocation of subscriber certificate:

1. GDCA or Registration Authority can revoke one subscriber certificate based on the requirements of this CP section 4.9.1.
2. For individual certificate, certificate subscribers can submit a request to revoke their own individual certificates.
3. For organization certificate, only representative authorized by this organization has the right to submit a request to revoke certificate which has been issued to this organization.
4. For equipment certificate, only representative authorized by this organization who has the equipment has the right to submit a request to revoke certificate which has been issued to this organization.
5. The court, government departments and other public power department can revoke subscriber certificate in accordance with the law.
6. Relying parties, application software suppliers, anti-virus organizations and other third parties may submit certificate problem reports informing GDCA of reasonable grounds to revoke the certificates.

只有 GDCA 可以撤销根证书或者中级 CA 证书。

Only GDCA can revoke root certificate or Subordinate CA certificate.

4.9.3. 证书撤销请求的处理程序 Procedure for Revocation Request

4.9.3.1. 订户请求撤销证书 The subscriber actively proposed to revocation application.

1. 订户向注册机构提交撤销，同时说明撤销原因；
2. 注册机构核实申请撤销实体的身份和撤销理由的正当性；
3. 注册机构将撤销申请表提交给 GDCA，由 GDCA 完成撤销；
4. GDCA 提供 7*24 小时的撤销申请服务。

1. Subscriber submits revocation application form and identification material to registration authority and indicates revocation reason.
2. Registration Authority verifies the identity of entities applying for revocation and the appropriateness of revocation reasons.
3. RA submits application form of revocation to GDCA and GDCA completes the revocation operation.
4. GDCA offers 24x7 certificate revocation requests service.

4.9.3.2. 订户被强制撤销证书 The subscriber is forced to revoke the certificate

1. 当 GDCA 或注册机构有充分的理由确信出现本 CP 第 4.9.1.1 节中的情况时，可通过内部

确定的流程撤销证书；

2. GDCA 提供 7*24 小时的证书问题报告和处理流程；
3. 当依赖方、司法机构、应用软件提供商、防病毒机构等第三方提请证书问题报告时，GDCA 应组织调查并根据调查结果来决定是否撤销证书；
4. GDCA 撤销订户证书后，通过适当的方式，包括电子邮件、电话等，告知订户证书已被撤销及撤销理由。

1. When GDCA or RA has sufficient reasons to confirm that circumstances described in CP section 4.9.1.1 have occurred, they can revoke subscriber certificates through determined internal processes;
2. GDCA maintains a 24x7 certificate problems reporting and processing procedures;
3. GDCA will take actions to investigate the certificate problem reports submitted by relying parties, judicial institutions, application software providers, anti-virus organizations and other third parties, and will decide whether or not to revoke the certificates based on the results of the investigation;
4. After the certificate revocation, GDCA or RA will use appropriate ways, including email, phone, and fax to notify the final subscriber that the certificate has been revoked and the reason why it is revoked.

4.9.4. 撤销请求的宽限期 Revocation Request Grace Period

如果出现密钥泄露或有泄露嫌疑等事件，撤销请求必须在发现泄密或有泄密嫌疑 8 小时内提出。其他撤销原因的撤销请求必须在变更的 48 小时内提出。

If key exposure occurs or suspected occurs, revocation request must be submitted in finding leakage or leakage suspicion within 8 hours after key exposure or suspected exposure is found. Revocation requirements caused by other reasons must be made within 48 hours.

4.9.5. CA 处理撤销请求的时限

Time Within Which CA Must Process the Revocation Request

GDCA 自接到撤销请求到完成撤销之间的间隔期限，不得超过 24 个小时。

The cycle of GDCA processes revocation request is no more than 24 hours.

4.9.6. 依赖方检查证书撤销的要求

Revocation Checking Requirements for Relying Parties

依赖方在依赖一个证书前必须查询 GDCA 发布的 CRL 确认他们所信任的证书是否被撤

销。

Relying parties must check the CRL published by GDCA before trusting a certificate to check whether the certificate is revoked.

4.9.7. CRL 发布频率 CRL Issuance Frequency

对于由 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 所签发的订户证书，CRL 发布周期为 8 小时。

对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的订户证书，CRL 发布周期为 24 小时，且 nextUpdate 字段的值不超出 thisUpdate 值的 10 天以上。

对于中级 CA 证书，GDCA 的 CRL 发布周期为 12 个月。如果撤销中级 CA 证书，GDCA 在撤销后 24 小时之内更新 CRL，且 nextUpdate 字段的值不得超出 thisUpdate 值的 12 个月以上。

在特殊紧急情况下可以使 CRL 立即生效（假使网络传输条件能够保证），CRL 的立即生效由 GDCA 制定的发布策略决定。

The subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, the CRLs are issued every 8 hours.

For the subscriber certificates issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT, 数安时代 R5 根 CA 证书, and GDCA TrustAUTH E5 ROOT, the CRLs are issued every 24 hours and the value of the nextUpdate field is not more than ten days beyond the value of the thisUpdate field.

For the subordinate CA certificates, GDCA shall update and publish certificate revocation list (CRL) every 12 months. In case the subordinate CA certificates are revoked, GDCA shall update and publish the certificate revocation list (CRL) within 24 hours after the revocation, and the value of the nextUpdate field shall be no more than twelve months beyond the value of the thisUpdate field.

However, CRL can come into effect immediately determined by release strategy made by GDCA in special emergency circumstances (assuming that the network transmission condition can guarantee).

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

一个证书从它被撤销到它被发布到 CRL 上的滞后时间不能超过 24 小时。

A revoked certificate will be added to CRL within 24 hours.

4.9.9. 在线状态查询的可用性 Online Revocation/Status Checking Availability

GDCA 应向证书订户和依赖方提供在线证书状态查询服务。OCSP 响应须符合 RFC 6960 的要求，并且被 OCSP 服务器签名。OCSP 服务器的证书与正在查询状态的证书由同一个 CA 签发，OCSP 服务器的证书应包含一个 RFC6960 定义的类型为 id-pkix-ocsp-nocheck 的扩展项。

GDCA should support OCSP responses for subscribers and the relying parties. The OCSP responses should conform to RFC 6960, and signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. The OCSP signing certificates should contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10. 在线状态查询要求 Online Revocation Checking Requirements

用户可以自由进行在线状态查询，GDCA 不得设置任何的读取权限。

GDCA 提供 Get 和 Post 两种方式的 OCSP 查询服务。

对于订户证书，GDCA 应至少每四天更新 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。

对于中级 CA 证书，GDCA 应至少每 12 个月更新 OCSP 信息。当撤销中级 CA 证书时，应在 24 小时内更新 OCSP 信息。

对于未签发的证书的状态查询请求，GDCA 不得返回“good”状态。

Users may feel free to inquire status online. GDCA must not impose any access limits.

GDCA offers the OCSP service using both the Get and Post methods.

For subscriber certificates, GDCA should update the OCSP information at least every four days. OCSP responses from this service have a maximum expiration time of ten days. For the revoked certificates, OCSP status will be updated immediately.

For subordinate CA certificates, GDCA should update the OCSP information at least every twelve months, and within 24 hours after revoking a subordinate CA certificate.

GDCA must not respond with a "good" status for the request for status of a certificate that has not been issued.

4.9.11. 撤销信息的其他发布形式

Other Forms of Revocation Advertisements Available

除了 CRL、OCSP 外，GDCA 可以提供撤销信息的其他发布形式，但这不是必须的。

GDCA may provide other publication forms of revocation information in addition to CRL and OCSP, however, such publication forms are not mandatory.

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

除本 CP 第 4.9.1 节规定的情形外，当订户或注册机构的证书密钥受到安全损害时，应立即向 GDCA 提出证书撤销请求。如果 CA 的密钥（根 CA 或中级 CA 密钥）安全被损害或者怀疑被损害，应该在合理的时间内用合式的方式及时通知订户和依赖方。

Except for the case described in CP section 4.9.1, when certificate key of subscriber or RA has security damages, certificate revocation request should be made to GDCA immediately. If CA key (root CA or Subordinate CA key) is compromised or may have been compromised, subscriber and relying party shall be notified by reasonable means timely.

证书订户以外的第三方可根据本 CP 的第 1.5.2.1 章中的联系方式，针对由 GDCA 签发的且未被撤销及未过期的证书，向 GDCA 发出证书密钥泄露的报告，报告方须使用以下方法之一证明持有或控制该证书对应的私钥：

- 提交由被泄露的私钥签名的 CSR，并在通用名项中添加“Proof of Key Compromise for GDCA”；或
- 直接提供被泄露的私钥。

GDCA 可酌情在本章节增加其他证明私钥泄露的方法。

Non-subscriber third parties may report a key compromise of an unexpired, unrevoked GDCA certificate according to the contact information described in section 1.5.2.1, using one of the following methods to prove possession/control of the private key associated with a certificate.

- Submission of a CSR signed by the compromised private key with the Common Name “Proof of Key Compromise for GDCA”; or
- Providing the private key itself.

GDCA may allow additional, alternative methods that do not appear in this section at its own discretion.

4.9.13. 证书挂起的情形 Circumstances for Suspension

GDCA 不支持证书挂起。

GDCA does not support certificate suspension.

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

GDCA 不支持证书挂起。

GDCA does not support certificate suspension.

4.9.15. 挂起请求的程序 Procedure for Suspension Request

GDCA 不支持证书挂起。

GDCA does not support certificate suspension.

4.9.16. 挂起的期限限制 Limits on Suspension Period

GDCA 不支持证书挂起。

GDCA does not support certificate suspension.

4.10. 证书状态服务 Certificate Status Services

4.10.1. 操作特征 Operational Characteristics

订户可以通过 CRL、LDAP 目录服务、OCSP 查询证书状态，上述方式的证书状态服务应该对查询请求有合理的响应时间和并发处理能力。

对于被撤销的证书，GDCA 不应在证书到期前删除其在 CRL 中的撤销记录。GDCA 不删除 CRL 中代码签名证书的撤销记录。

GDCA 不删除 OCSP 中的撤销记录。

Subscribers can query certificate status through the CRL, LDAP and OCSP. Certificate status services described above should have reasonable response time and concurrency process capability for query request.

For the revoked certificates, GDCA shall not remove their revocation records from CRL prior to expiration of such certificates. GDCA does not remove the revocation records of code signing certificates from the CRL.

GDCA does not remove the revocation records in the OCSP.

4.10.2. 服务可用性 Service Availability

证书状态服务必须保证 7X24 小时可用，且响应时间不得超过 10 秒。

Certificate Status Services must be available in 24 × 7 hours, and the response time must be of ten seconds or less.

4.10.3. 可选特征 Operational Features

不适用。

Not applicable.

4.11. 订购结束 End of Subscription

订户证书出现下列情形时表明订户的订购行为正式结束：

The following circumstances of certificates indicate that the subscriber's subscribing behavior has formally terminated:

1. 证书到期后没有进行更新；

1. The certificate is not renewed after the expiration.

2. 证书到期前被撤销。

2. The certificate is revoked before the expiration.

4.12. 密钥托管与恢复 Key Escrow and Recovery

4.12.1. 密钥托管与恢复的策略与行为

Key Escrow and Recovery Policy and Practices

对于由 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 所签发的订户证书：证书订户的加密密钥对由 GDCA 代订户 GDCA 申请生成，并由 GDCA 进行管理。当证书订户认为需要恢复加密密钥时，可以向 GDCA 提出申请恢复加密密钥，GDCA 按照规范、流程，接受订户的申请，为订户恢复相应的加密密钥。

证书订户的签名密钥对由订户自行保管，GDCA 不接受订户签名密钥的托管和恢复。

For the subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1:The encryption key pair of the subscriber is applied for and generated by the GDCA on behalf of the subscriber, and is managed by the GDCA. When the subscriber needs to recover the encryption key, they can submit an application to GDCA for key recovery. GDCA will process the subscriber's application and recover the corresponding encryption key for the subscriber according to the established procedures.

Subscribers shall keep signing key pairs by themselves. GDCA does not provide the key escrow and recovery services for subscribers' signing key pairs.

对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的订户证书：订户的密钥对由订户自行生成。如果密钥对由加密硬件保存，GDCA 要求订户必须使用满足或超过 FIPS 140-2 第二级别要求的加密硬件妥善保管私钥，始终保持对私钥的唯一控制。订户可以委托 GDCA 代订户进行生成密钥对和 CSR。因私钥遗失、泄露等所造成的损失由订户自己承担，GDCA 对此不承担责任。GDCA 不提供订户私钥的托管和恢复服务。

For subscriber certificates issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA 证书 and GDCA TrustAUTH E5 ROOT: The key pairs of subscribers shall be generated by the subscribers themselves. In case the key pairs are to be stored in a cryptographic hardware, GDCA requires that the subscribers must use cryptographic hardwares that meet or exceed the requirements of FIPS 140-2 level 2 to properly keep the private keys, and must always keep unique control of the private keys. Subscribers can authorize GDCA to generate key pairs and CSR. Subscribers shall undertake the responsibilities by themselves for the losses incurred by the loss of signature private key, and GDCA refuses to take the corresponding responsibilities.

GDCA does not provide key escrow and recovery services for the subscribers' private keys.

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

非对称算法组织数字信封的方式来封装会话密钥，数字信封使用信息接受者的公钥对会话密钥加密，接受者用自己的私钥解密并恢复会话密钥。

The session key is packaged in digital envelope using asymmetric algorithm. The digital envelope is to encrypt the session key using information recipient's public key, then the recipient can use their own private key to decrypt and recovery the session key.

5. 认证机构设施、管理和操作控制

Facility, Management, and Operational Controls

5.1. 物理控制 Physical Controls

5.1.1. 场地位置与建筑 Site Location and Construction

GDCA 中心机房按照功能主要分为核心区、服务区、管理区、操作区、公共区五个区域。核心区是一个高性能电磁屏蔽室。其壳体是六面优质冷轧钢板，其中顶、墙板采用厚度为 2mm

的冷轧钢板，地板采用厚度为 3mm 的冷轧钢板。焊接工艺为 CO2 保护焊。玻璃是加厚的嵌有金属网的防弹玻璃。屏蔽门是手动锁紧屏蔽门。通风口是按屏蔽室规格配置蜂窝型通风波导窗。电源滤波器是单相高性能低泄漏滤波器。存放保密资料的密码柜必须放置在核心区。

According to the functions of GDCA central area, it consists of core area, service area, management area, operation area, public area. The core area is a high-performance electromagnetic shielding room. Its shell is made of six sides of high quality cold-rolled steel plate. The roof and wall panel is made of cold-rolled steel plate with thickness of 2 mm. The floor is made of cold-rolled steel sheet with thickness of 3 mm. Welding process is CO2 protection welding. Glass is thickened and bulletproof with metal mesh added on it. Shielding door is manual locked. Vent is configured with honeycomb type ventilation duct shielding room window according to the specifications of the shielding room. Power filter is single phase high-performance low leakage filter. Safe with confidential information stored must be placed in the core area.

5.1.2. 物理访问控制 Physical Access

进出每一个物理安全层的行为都需要被记录、审计和控制，从而保证进出每一个物理安全层的人都是经过授权的。GDCA 的 CPS 必须对物理访问控制进行比较详细的规定。

The activities of accessing to each physical security layer shall be recorded, audited and controlled in order to ensure that all above activities of certain person have been authorized. GDCA CPS must define detailed rules for physical access control.

5.1.3. 电力与空调 Power and Air Conditioning

GDCA 机房应有安全、可靠的电力供电系统及电力备用系统，以确保持续不间断的电力供应。另外，还应具有机房专用空调系统、新风系统控制运营设施中的温度和湿度。

The computer room of GDCA shall be equipped with secure and reliable electric power system and electric backup system to ensure continuous, uninterrupted access to electric power. In addition, these systems shall have temperature and relative humidity of special air-conditioning system and wind system control operation facilities.

5.1.4. 防水 Water Exposures

GDCA 机房应有专门的技术措施，防止、检测漏水的出现，并能够在出现漏水时最大程度地减小漏水对认证系统的影响。

The computer room of GDCA should have specialized technical measures to prevent and detect leaks, and be able to reduce the influence of leakage on the certification system to the maximum extent.

5.1.5. 火灾防护 Fire Prevention and Protection

GDCA 机房应采取预防措施，并制定相应的程序来消除和防止火灾的发生，这些火灾防护措施应符合当地消防管理部门的安全要求。

The room of GDCA should take preventive measures, and formulate the corresponding program to eliminate and prevent the occurrence of the fire. These measures shall meet local applicable safety regulations.

5.1.6. 介质存放 Media Storage

对物理介质的存放和使用应满足防火、防水、防震、防潮、防腐蚀、防虫害、防静电、防电磁辐射等的安全需求，并且建立严格的保护手段以防止对介质未经授权的使用和访问。

GDCA meets the security requirements for media storage, including fire-proof, water-proof, earthquake-proof, moisture-proof, corrosion-proof, pest-proof, static-proof, electromagnetic radiation-proof, etc. Meanwhile, GDCA takes strict measures to prevent the media from unauthorized use and access.

5.1.7. 废物处理 Waste Disposal

当 GDCA 存档的纸张文件和材料已不再需要或存档期限已满时，必须采取措施销毁，使信息无法恢复。密码设备和存放敏感信息的存储介质在作废处置前根据制造商提供的方法先将其初始化并进行物理销毁。

The written documents and materials of GDCA should be destroyed when they are no longer needed or exceeded the expiration date, and must not be recovered. Cryptographic devices and media with sensitive information should be initialized and physically destroyed by using manufacturer’s method before disposal.

5.1.8. 异地备份 Off-Site Backup

GDCA 建立了异地数据备份中心，使用专门的软件对关键系统数据、审计日志数据和其他敏感信息进行异地每天备份。

GDCA has established a remote data backup center. It backups the core system data, audit log data and other sensitive information by the specialized software at off-site location on a daily basis.

5.2. 程序控制 Procedural Controls

5.2.1. 可信角色 Trusted Roles

在 GDCA 提供的电子认证服务过程中，能从本质上影响证书的颁发、使用、管理和撤销等涉及密钥操作的职位都被 GDCA 视为可信角色。这些角色应包括：

In the process of electronic authentication service provided by GDCA, a person who can essentially affect the processes of certificate issuance, usage, management and revocation, and other related positions which are involved in key operation is considered as trusted roles. The trusted roles include:

1. 密钥和密码设备的管理人员；

1. Administrator of key and password devices.

2. 系统管理人员；

2. System administrator.

3. 安全审计人员；

3. Security auditor.

4. 业务管理人员及业务操作人员。

4. Business administrator and business operator.

5.2.2. 每项任务需要的人数 Number of Persons Required per Task

GDCA 应在具体业务规范中对关键任务进行严格控制，确保多个可信角色共同参与完成一些敏感的任务：

GDCA should strictly control key task for specific business specification to ensure that various trusted roles jointly participate in completeness of some sensitive tasks:

1. 密钥和密码设备的操作和存放：需要 5 个可信人员中的 3 个共同完成；
2. 证书签发系统的后台操作：需要 3 个系统管理人员中的 2 个可信人员共同完成；
3. 审核和签发证书：需要 2 个可信人员共同完成。

1. For operation and storage of the key cryptographic equipment, it requires at least three of five trusted persons to operate.
2. For background operation of the certificate issuance system, it requires at least two of three trusted persons to operate.
3. For review and issuance of the certificate, it requires two trusted persons to operate.

5.2.3. 每个角色的识别与鉴别 Identification and Authentication for Each Role

对于所有承担可信角色的人员，必须进行严格的识别和鉴证，确保其能够满足所从事工作职责的要求。鉴证程序在 GDCA 的人员聘用管理条例中规定。

All persons who undertake trusted roles must be identified and authenticated strictly to ensure that they can meet the requirements of their jobs. The identification procedure is given in the GDCA personnel management regulations.

5.2.4. 需要职责分割的角色 Roles Requiring Separation of Duties

所谓职责分割，是指如果一个人担任了某一职能的角色，就不能再担任另一特定职能的角色。需要职责分割的角色包括且不限于：

Segregation of duties means a person who plays a specific role cannot be the person who plays another specific role. Roles requiring segregation of duties include but not limit to:

1. 证书业务受理
2. 证书或 CRL 签发
3. 系统工程与维护
4. CA 密钥管理
5. 安全审计

1. The acceptance of the certificate businesses
2. The issuance of certificates or CRLs
3. System Engineering and Maintenance
4. CA key management
5. Security auditing

5.3. 人员控制 Personnel Controls

5.3.1. 资格、经历和清白要求 Qualifications, Experience, and Clearance Requirements

GDCA 对承担可信角色的工作人员的资格要求如下：

1. 具备良好的社会和工作背景；
2. 遵守国家法律、法规，服从 GDCA 的统一安排及管理；

3. 遵守 GDCA 有关安全管理的规范、规定和制度；
4. 具有良好的个人素质、修养以及认真负责的工作态度；
5. 具备良好的团队合作精神。
6. 无违法犯罪记录。

The qualification requirements of person who undertakes trusted role in GDCA are as follows:

1. Good social and working background.
2. Complying with state's laws and regulations. Obeying GDCA's unified arrangement and management.
3. Complying with the GDCA related security management norms, regulations and specifications.
4. Having good personalities and working attitudes, with good working experience.
5. A good team player.
6. No illegal and criminal records.

GDCA 要求充当可信角色的人员至少必须具备忠诚、可信赖及对工作的热诚、无影响 CA 运行的其它兼职工作、无同行业重大错误记录等。

A person required by GDCA as trusted role personnel must have loyalty, trustworthiness and dedication to work, without other part-time work that affects CA daily operation, no major bad records of this industry and etc.

5.3.2. 背景调查程序 Background Check Procedures

GDCA 与有关的政府部门和调查机构合作，完成对可信员工的背景调查。

GDCA collaborates with governments and investigation organizations to complete background review for the trusted roles.

所有的可信员工和申请调入的可信员工都必须书面同意对其进行背景调查。背景调查分为：基本调查和全面调查。

All employees who are trusted or apply for should have a written consent that they must go through a background investigation. Background review including: basic review and full review.

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。

Basic review includes reviewing work experience, job recommendation, education and social relation.

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。对于公开信任证书业务的关键岗位必须进行全面调查。

Full review includes reviewing criminal records, social relation and social security besides basic review. Full reviews must be carried out for key roles that involve with publicly trusted certificates business.

调查程序包括：

a) 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。

b) 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。

c) 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。

d) 经考核，GDCA 与员工签订保密协议，以约束员工不许泄露 CA 证书服务的所有保密和敏感信息。同时，GDCA 还将按照本机构的人员管理相关条例对所有承担可信角色的在职人员进行职位考察，以便能够持续验证这些人员的可信程度和工作能力。

The review procedure includes:

a) The HR department is responsible for confirming candidate's personal information. Candidates should provide the following information: resume, the highest degree graduation certificate, degree certificate, qualification certificate and identity card and other related valid certificates.

b) The HR department identifies the authenticity of the information provided by candidates through telephone, correspondence, network, visits and other forms.

c) The HR department checks candidates through on-site assessment, daily observation, situational test and other methods.

d) After the review, GDCA signs a confidentiality agreement with employee in order to restrain employee not to reveal any confidential and sensitive information of CA certificate services. At the same time, GDCA will also be in accordance with the relevant organization regulations of personnel management and make job examination on in-service staff who assumed trusted role, so as to continuously review these employees' trustworthiness and working ability.

5.3.3. 培训要求 Training Requirements

为了使员工能够胜任工作，需要对员工进行必要的岗前培训和工作中的再培训，以更好的满足工作岗位对人员的要求。培训应该包括但不限于以下内容：

In order to make the employees to be competent at his/her jobs, pre-training and re-training must be conducted for employees to meet the requirements of the job positions. Content of training shall include but not limit to:

1. GDCA 颁布的证书策略和电子认证业务规则；

1. CP and CPS issued by GDCA.

2. PKI 基本知识；

2. PKI basic knowledge.

3. 电子签名法和相关法律法规；

3. Electronic Signature Law of the People's Republic of China related laws and regulations.

4. GDCA 运营体系、技术体系和安全管理制度；

4. GDCA operation system, technology system and security management system.

5. 工作职责和岗位说明。

5. Working responsibility and job description.

5.3.4. 再培训的频度和要求 Retraining Frequency and Requirements

GDCA 应根据需要安排再培训，以保证重要岗位的员工更加符合岗位需求，顺利地完成其工作职责。

GDCA shall arrange for continuous re-training for employees at important positions regularly to ensure employees can meet their job requirements and complete their jobs more smoothly.

5.3.5. 工作岗位轮换的频度和次序 Job Rotation Frequency and Sequence

GDCA 应依据安全管理策略制定在职人员的工作岗位轮换周期和顺序。

Job rotation cycle and the sequence of GDCA serving officer will be based on organization security management strategy.

5.3.6. 未授权行为的处罚 Sanctions for Unauthorized Actions

GDCA 应建立并维护一套管理办法，对未授权行为进行适当的处罚，包括解除或终止劳动合同、调离工作岗位、罚款、批评教育、提交司法机构处理等方式。这些处罚行为应当符合法律法规的要求。

GDCA shall establish and maintain a set of measures for the administration, including termination of labor contracts, position removing, fines, criticism and education, submitting to Judiciary for processing, etc., to appropriately discipline the personnel unauthorized activities. Above discipline activities shall comply with laws and regulations.

5.3.7. 独立合约人的要求 Independent Contractor Requirements

对于不属于 GDCA 机构内部工作人员，但从事 GDCA 业务有关工作的如业务分支机构的业务人员、管理人员等独立合约人，GDCA 的统一要求如下：

1. 人员档案的备案管理；
2. GDCA 提供统一的岗前培训和工作中的再培训，培训内容包括但不限于 GDCA 证书受理规则和电子认证业务规则。

For persons who do not belong to the GDCA but participate in the relevant works for GDCA businesses, such as business personnel of business branch organization, management personnel and other independent contractors, GDCA has requirements are as follows:

1. Record management of personnel profiles
2. GDCA provides unified training and retraining, includes but not limited to the GDCA certificate acceptance rules and electronic certification business rules.

5.3.8. 提供给人员的文件 Documentation Supplied to Personnel

GDCA 提供给内部员工的文件应包括培训材料和与员工工作相关文档。

Documents provided to internal employees by GDCA include training documents and related personnel working documents.

5.4. 审计记录程序 Audit Logging Procedures

5.4.1. 记录事件的类型 Types of Events Recorded

CA 和 RA 必须记录与运行系统相关的事件，可在必要时供合格审计师查看。这些记录，无论是手动生成或者是系统自动生成，都应该包含以下信息：

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。

All major security incidents occurred in GDCA will be logged in the audit trail records, and will be made available to qualified auditors for review when necessary. Regardless of manual or automatic generation, these records should contain the following information:

1. The date and time of the event
2. Sequence number for the record
3. Type of record
4. Record source
5. Event recording entity

GDCA 应记录的事件包括但不限于：

1. CA 密钥生命周期内的管理事件，包括 CA 密钥生成、备份、存储、恢复、使用、撤

销、归档、销毁、私钥泄露等；

2. 证书生命周期内的管理事件，包括证书的申请、批准、更新、撤销等；
3. 系统、网络安全事件，包括：成功或失败的访问 CA 系统的活动，系统日常运行产生的日志文件，系统变更等；
4. 信息安全设备的安全事件：路由器和防火墙活动的日志记录至少应包括以下内容：1）记录所有成功和失败的路由器及防火墙登录尝试；2）记录所有在路由器和防火墙上执行的管理操作，包括配置更改、固件更新以及访问控制修改；3）记录所有防火墙规则的更改，包括新增、修改和删除；4）记录所有系统事件和错误，包括硬件故障、软件崩溃以及系统重启；
5. 系统操作事件，包括系统权限的创建、删除，设置或修改密码；
6. 认证机构设施的访问，包括授权人员进出认证机构设施、非授权人员进出认证机构设施等相关记录；
7. 可信人员管理记录，包括系统权限的创建、删除及变更等。

These events include but not limited to:

1. Management events in key's life cycle, including generation, backup, storage, recovery, usage, revocation, archiving, destruction, private key leakage, etc.
2. Management events of certificate life cycle, including application, approval, update, revocation, etc.
3. System and network security events including: successful or unsuccessful access attempts for CA system, logs generated during the daily system operation and system updates etc.
4. Security events recorded via information security devices: Logging of router and firewall activities at a minimum include: 1) Successful and unsuccessful login attempts to routers and firewalls; and 2) Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and 3) Logging of all changes made to firewall rules, including additions, modifications, and deletions; and 4) Logging of all system events and errors, including hardware failures, software crashes, and system restarts.
5. System operating events, creation or deletion of permission, configuration or modification of password.
6. Access to CA facilities, including the access of authorized or unauthorized personnel and attendants, and other relevant records.
7. Management record of trusted roles and personnel, including system access application, deletion and modification.

5.4.2. 处理日志的频度 Frequency of Processing Log

GDCA 应定期检查审计日志，以便发现重要的安全和操作事件，对发现的安全事件采取

相应的措施。

All the audit logs should be checked by GDCA regularly in order to discover the significant security and operation events and take corresponding measures.

5.4.3. 审计日志的保留期限 Retention Period for Audit Log

GDCA 必须妥善保存电子认证服务的审计日志，保存期限为电子签名认证失效后五年。

GDCA saves electronic certification service audit logs properly. The preservation limitation period is five years after the date of expiration of the electronic signature certification.

5.4.4. 审计日志的保护 Protection of Audit Log

所有的审计日志，应当采取严格的物理和逻辑访问控制措施，防止未经授权的浏览、修改、删除等。

All the audit logs should be handled with strict physical and logical access control measures to avoid unauthorized reading, modification and deletion, etc.

5.4.5. 审计日志的备份程序 Audit Log Backup Procedures

对审计日志的备份应该建立和执行可靠的制度，定期进行备份。

GDCA should set up and carry out the reliable system for backups of audit logs, and full backups are performed periodically.

5.4.6. 审计收集系统 Audit Collection System (Internal vs. External)

不适用。

Not applicable.

5.4.7. 对导致事件主体的通知 Notification to Event-Causing Subject

审计记录报告一个事件时，应通知引起该事件的个人、组织机构。

When audit record reports an event, GDCA shall notify individuals, organizations who cause this event.

5.4.8. 脆弱性评估 Vulnerability Assessments

根据审计记录，GDCA 应定期进行安全脆弱性评估，并根据评估报告采取补救措施。

GDCA should conduct security vulnerability assessments regularly according to audit records and take remedial measures according to assessment reports.

5.5. 记录归档 Records Archival

5.5.1. 归档记录的类型 Types of Records Archived

需要归档的记录，除了本 CP 第 5.4.1 节规定的外，还需要对如下记录进行归档，包括：

In addition to the records need to be archived specify in CP section 5.4.1, the following records should be archived:

1. 证书申请信息；

1. Information of certificate application.

2. 证书签发过程中的支持文档。

2. Supporting documents of certificate issuance.

5.5.2. 归档记录的保留期限 Retention Period for Archive

GDCA 的电子认证业务规则（CPS）应规定合理的归档记录保留期限。

CPS of GDCA shall provide reasonable retention period for archive.

5.5.3. 归档文件的保护 Protection of Archive

应通过适当的物理和逻辑的访问控制方法保护归档数据，只有授权的可信人员允许访问归档数据，防止未经授权的浏览、修改、删除或其它的篡改行为。

All archive records shall take appropriate measures to control physical and logical access so that only trusted personnel can access records. Archive records shall be protected from the unauthorized browsing, modifying, deleting and other illegal operations.

5.5.4. 归档文件的备份程序 Archive Backup Procedures

对于系统生成的电子归档记录，应当定期进行备份，备份文件进行异地存放。

Electronically archived records generated by the systems should be backed up weekly. The backup file should also be stored off-site.

对于书面的归档资料，不需要进行备份，但需要采取严格的措施保证其安全性。

For the written archiving data, they do not need to be backed up, but some strict measures need to be taken to ensure the security.

5.5.5. 记录时间戳要求 Requirements for Time-Stamping of Records

GDCA 的所有日志都有时间记录，均由操作人员手工记录或系统自动添加。

All the GDCA records are labelled with time, and the time will either be added manually by the operators or automatically by system.

5.5.6. 归档收集系统 Archive Collection System (Internal or External)

各自实体应在内部建设归档收集系统，包括 GDCA 和注册机构。

All the entities including GDCA and RA should construct internal archive collection system.

5.5.7. 获得和检验归档信息的程序

Procedures to Obtain and Verify Archive Information

GDCA 的安全审计员和运维人员分别保留归档信息的 2 个拷贝。在获得完整归案信息时，须对这 2 个拷贝进行比较。

Security auditors and operation and maintenance team of GDCA retain 2 copies of the GDCA file information respectively. While obtaining the complete archived information, comparison of the 2 copies should take place to confirm the integrity.

5.6. 密钥变更 Key Changeover

在 CA 证书到期时，GDCA 将对 CA 证书进行更新。只要 CA 密钥对的累计寿命没有超过本 CP 第 6.3.2 节中规定的最大生命期，那么 CA 证书可以使用原密钥进行更新。否则需要产生新的密钥对，替换已经过期的 CA 密钥对。即使在密钥对生命期内，GDCA 也可以通过生成新密钥对的方式产生新的 CA 证书。在一个 CA 证书过期之前，密钥变更过程被启动，以保障这个 CA 体系中的实体从 CA 旧密钥对到新密钥对的平稳过渡。

When the certificate of CA expires, GDCA will renew the certificate of CA. As long as CA key pair does not exceed the maximum lifetime specified in Section 6.3.2, the certificate of CA could renew using original key. Otherwise, new key pair shall be generated to replace the expired key pairs of certificate of CA. Also, even in the key pair life cycle, GDCA could generate new certificate of CA by using new key pair. Before the certificate of former level CA expires, key changeover shall be performed to ensure that the entities in the CA system shall switch from original key pair to new key pair smoothly.

在生成新的 CA 密钥对时，必须严格遵守 GDCA 关于密钥管理的规范。新的密钥对产生时，GDCA 将签发新的 CA 证书，并及时进行发布，让订户和依赖方能够及时获取新的 CA

证书。

New CA key pair is generated according to the key management rules of GDCA strictly. While generating new key pair, GDCA shall issue and publish the new CA certificate timely, and it shall be available for subscriber and relying party to obtain new CA certificate.

CA 密钥更替时，必须保证整个证书链的顺利过渡。

Make sure that the entire certificate chain transits smoothly in CA key changeover.

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

GDCA 应制订各种事故处理方案和应急处理预案，规定相应的事故和损害处理程序。

GDCA should make handling schemes of different kinds of accidents and handling pre-scheme of emergency, stipulate corresponding handling procedures of accidents and damages.

5.7.2. 计算机资源、软件和/或数据的损坏

Computing Resources, Software, and/or Data Are Corrupted

如果出现计算机资源、软件和/或数据损坏的事件，GDCA 立即启动事故处理程序，如有必要，可按照灾难恢复计划实施恢复。

Following corruption of computing resources, software, and/or data, GDCA shall utilize the incident and compromise handling procedures promptly. If necessary, the disaster recovery procedures could be used.

5.7.3. 实体私钥损害处理程序 Entity Private Key Compromise Procedures

在故意的、人为的或是自然灾难的情况下，GDCA 将采取下列步骤以恢复安全环境：

1. GDCA 认证系统的口令由业务管理员、业务操作员、系统管理员进行变更；
2. 根据灾难的性质，部分或全部证书需要撤销或之后重新认证；
3. 如果目录无法使用或者目录有不纯的嫌疑，目录数据，加密证书和 CRL 需要进行恢复；
4. 及时访问安全现场尽可能合理地恢复操作；
5. 如果需要恢复业务管理员的配置文件，应由系统管理员执行恢复；
6. 如果需要恢复 GDCA 业务操作员的配置文件，则由另外一名 GDCA 安全业务操作员或业务管理员对其进行恢复。

In case of any intentional, man-made or natural disasters, GDCA will take the following steps to restore security environment:

1. GDCA verification system's password is changed by the business administrator, business operators and system administrator.
2. According to the type of disaster, some or all certificates will be revoked or re-verified later.
3. Directory data, encryption certificate and CRL are needed for recovery if the directory is unavailable or directory with impure suspicion.
4. Timely access to security site as far as possible to restore operation reasonably.
5. While restore the business administrator's configuration file, it will be done by the system administrator.
6. While restore the GDCA business operator's configuration file, it will be done by another GDCA security business operator or administrator.

当 CA 根私钥被攻破或泄露，GDCA 启动重大事件应急处理程序，由安全策略委员会和相关的专家进行评估，制定行动计划。如果需要注销 CA 证书，将会采取以下措施：

When CA root private key has been damaged, missed, tampered or leaked, GDCA starts a major emergency treatment process, which is assessed by GDCA Security Policy Committee and the relevant experts to make a plan. If the CA certificate must be revoked, the following measures will be taken:

1. 告知依赖方和国家主管部门；

1. Notify relying parties and state administrative department.

2. 发布证书注销状态到信息库；

2. Publish certificate revocation status to repositories.

3. 通过 GDCA 网站或其它通信方式发布关于注销 CA 证书的处理通报；

3. Publish handling notification about revoked certificates at GDCA website or by other communication methods.

4. 产生新的根私钥，重新为订户签发证书。

4. Generate new root private key and re-issue certificate to subscriber.

5.7.4. 灾难后的业务存续能力 Business Continuity Capabilities After a Disaster

GDCA 在发生灾难后，应有如下几个方面的业务存续能力：

GDCA should have the following continuity capabilities after a disaster:

1. 在尽可能短的时间内恢复业务系统，最多不超过 48 小时；

1. Recover business system as soon as possible, not exceeding 48 hours.

2. 能够恢复客户信息；

2. Recover information of customers.

3. 能够保证恢复后的运营场地符合安全要求；

3. Ensure the operation site meets the security requirements after recovered.

4. 有足够的人员继续开展业务并且不违反职责分割的要求。

4. There are enough employees to operate the business and not violating segregation of duties.

5.8. CA 或 RA 的终止 CA or RA Termination

当GDCA及其注册机构需要停止其业务时，必须严格按照《中华人民共和国电子签名法》、《电子认证服务管理办法》及相关法规中对认证机构终止电子认证服务的规定要求进行有关工作。

When GDCA and its RA need to stop their business, it shall enforce termination procedures strictly according to “Electronic Signature Law of the People's Republic of China”, “Measures for the Administration of Electronic Certification Services” and relevant laws and regulations.

在 GDCA 终止前，必须：

1. 委托业务承接单位；
2. 起草 GDCA 终止声明；
3. 通知与 GDCA 终止相关的实体；
4. 关闭从目录服务器；
5. 证书注销；
6. 处理存档文件记录；
7. 停止认证中心的服务；
8. 存档主目录服务器；
9. 关闭主目录服务器；
10. 处理 GDCA 业务管理员和 GDCA 业务操作员的操作权限；
11. 处理加密密钥；
12. 处理和存储敏感文档；
13. 清除 GDCA 主机硬件。

Before termination, GDCA must:

1. Arrange the business to undertake
2. Draft GDCA termination statement
3. Notify the entities that are related to GDCA termination.
4. Shut down subordinate LDAP
5. Certificate revocation

6. Treatment of archive file record
7. Termination of certificate authority service.
8. Archive main LDAP
9. Shutdown main LDAP.
10. Dispose the access of GDCA business administrator and GDCA business operator.
11. Process encryption key.
12. Process and store sensitive documents.
13. Remove GDCA mainframe hardware

当 RA 因故终止服务时，GDCA 将按照与其签订的相关协议处理有关业务承接事宜和其他事项。

When RA terminates its services, GDCA deals with all the relevant business in accordance with the agreements.

6. 认证系统技术安全控制 Technical Security Controls

6.1. 密钥对的生成与安装 Key Pair Generation and Installation

6.1.1. 密钥对的生成 Key Pair Generation

6.1.1.1. CA 密钥对生成 Generation of CA Key Pair

CA 密钥对必须在安全的物理环境中，由多个可信人员在国家密码主管部门批准和许可的密码设备中生成。密钥的生成、管理、存储、备份和恢复应遵循 FIPS140-2 标准的相关规定。由于 FIPS140-2 标准并非是国家密码主管部门认可和支持的标准，国家对于密码产品有严格的管理要求，因此 FIPS140-2 标准仅参照执行，是在国家密码管理政策许可前提下的选择性适用，具体参照设备厂商提供的资料。用于此类密钥生成的密码模块须通过国家密码主管部门鉴定、认证。

CA 密钥对的生成过程需录像或由一名合格的审计师见证以确保其遵循 CP 以及角色分离的要求。密钥对生成过程和操作均需记录并保存。

The key pairs of CAs are generated within the cryptographic devices approved and licensed by OSCCA, in a physically secure environment and under the control of multiple trusted persons. The generation, management, storage, backup and recovery of the key pair shall comply with the relevant regulations of FIPS140-2 standard. Since FIPS140-2standard is not a standard that approved and accepted by OSCCA,

for strict manage requirements of state's cryptographic products, GDCA only takes the provisions of FIPS140-2 under the permission of OSCCA according to the information provided by device manufacturer. Hardware Security Module used for key generation must be authenticated and certified by OSCCA.

The generation of the CA key pairs shall be video recorded or witnessed by a qualified auditor to ensure the generation process complies with the requirements of this CP and follow the separation of roles principle. The procedures and operations related to key pair generation shall be recorded and archived.

6.1.1.2. 订户密钥对生成 Generation of Signing Key Pair

订户签名密钥对的产生，必须遵循国家的法律政策规定。GDCA 支持多种模式的签名密钥对产生方式，可以使用硬件密码模块（如：USB Key），也可以使用国家密码管理局批准的软件密码模块，也可以使用标准的软件密码模块（如：Web 服务器软件提供的密钥生成功能等），证书申请者可根据其需要进行选择，密钥长度至少为 RSA 2048 位或 ECC 256 位。对于第 4 类个人证书、第 4 类机构证书、代码签名证书，则必须使用硬件密码模块生成密钥。不管何种方式，密钥对产生的安全性都应该得到保证。GDCA 在技术、业务流程和管理上，已经实施了安全保密的措施。

The generation of the subscriber's signing key pairs must comply with the national laws and regulations. GDCA supports multiple patterns to generate signing key pair. Subscriber can use a hardware cryptographic module (such as USB Key), or software cryptographic module approved by OSCCA, or a standard software cryptographic module (such as the key generation function offered by web server software, etc.), so subscribers can choose according to their needs, and the key sizes are at least RSA 2048 or ECC 256. It must use the hardware cryptographic module to generate keys for type IV individual certificate type IV organization certificate and code signing certificates. In any case, the security of key pair's generation shall be guaranteed. GDCA shall implement adequate security measures in technology, business processes and management.

（1）对于由 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 所签发的订户证书：

订户在使用硬件密码模块时，必须使用国家密码管理局批准许可的设备生成签名密钥对，例如由密码机、密码卡、USB Key、IC 卡等生成。订户在选择这些设备前，应事先向 GDCA 咨询有关系统兼容和接受事宜。GDCA 向订户提供符合国家密码管理相关规定的设备作为订户签名密钥对的生成和存储设备。

GDCA 一般不提供代订户生成签名密钥对，如果用户书面申请并经 GDCA 批准，GDCA 可以为申请者代为生成密钥对，并且承诺不保留私钥的副本，采取足够的措施保证密钥对的安全性、可靠性和唯一性，但是由于此密钥对的遗失、泄露等原因造成的损失，GDCA 不承担任何责任与义务。

证书订户的加密密钥对由 GDCA 代订户申请生成，并由 GDCA 进行管理。当证书订户

需要恢复加密密钥时，按照 GDCA 流程，接受订户的申请为订户恢复相应的加密密钥。

For the subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1:

When using hardware cryptographic modules, subscribers must generate signing key pair with devices approved by OSCCA, such as cryptographic server, cryptographic card, USB Key and IC card etc. Before choosing of these devices, subscribers should consult with GDCA on system compatibility and acceptance. In addition，GDCA provides devices to subscribers as generation and storage devices of signing key pairs which are in accordance with the relevant provisions of state cryptography management.

Generally, GDCA does not provide signing key pairs for subscribers, unless when submit written applications to do so and approved by GDCA, and GDCA guarantees not to hold copy of private keys, and take effective actions to ensure the key pairs are safe, trustworthy and unique. However, GDCA does not assume any responsibilities and obligations for the losses caused by the loss, disclosure of such key pairs or for any other reason related to such key pairs.

The encryption key pair of the subscriber is applied for and generated by the GDCA on behalf of the subscriber, and is managed by the GDCA. When the subscriber needs to recover the encryption key, they can submit an application to GDCA for key recovery. GDCA will process the subscriber's application and recover the corresponding encryption key for the subscriber according to the established procedures.

（2）对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的订户证书：

对于 SSL/TLS 证书和时间戳证书，订户的密钥对由订户自己生成并保管。

对于邮件证书，GDCA 允许订户在线生成密钥对并将私钥加密保护后通过安全通道传送给订户，或由订户提交 CSR 签发证书。

对于符合 AATL 技术要求的证书及代码签名证书，由订户采用符合标准要求的硬件设备生成密钥对，私钥不能复制和导出，同时必须使用口令激活私钥，GDCA 通过安全通道将激活口令传递给订户。

证书订户负有保护私钥安全的责任和义务，并承担由此带来的法律责任。

在公钥对应于行业公认的弱私钥方面，对于 2024 年 11 月 15 日或之后提交的请求，GDCA 至少应采取以下预防措施：

1. 对于 Debian 弱密钥漏洞（https://wiki.debian.org/SSLkeys），GDCA 拒绝在 https://github.com/cabforum/Debianweak-keys/ 中列出的每种密钥类型（例如 RSA、ECDSA）和密钥长度的所有密钥。对于满足第 6.1.5 节要求的其他密钥，除 RSA 密钥长度超过 8192 位的情况外，GDCA 拒绝 Debian 弱密钥。

2.对于 ROCA 漏洞，GDCA 拒绝通过 https://github.com/crocs-muni/roca 或等效工具识别的密钥。

3.对于接近素数漏洞（https://fermatattack.secvuln.info/），GDCA 拒绝可通过 Fermat 分解方法在 100 轮内分解的弱密钥。

For subscriber certificate issued by subordinate CAs of GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA certificate and GDCA TrustAUTH E5 ROOT certificate:

For SSL/TLS certificates and timestamp certificates, subscribers' key pairs are generated and kept by the subscribers themselves.

For e-mail certificates, GDCA allows the subscribers to generate key pairs online and will deliver the encrypted private keys to the subscribers through secure channels. Subscribers may submit the CSR for the issuance of such certificates.

For the certificates that are compliant to the AATL Technical Requirements and the code signing certificates, subscribers shall use the hardware equipment that meets relevant requirements to generate key pairs, and private keys shall not be duplicated or exported, and the activation of which must require a password. GDCA will deliver the activation passwords to the subscribers through secure channels.

Certificate subscribers have the responsibilities and obligations to protect the security of private keys, and assume the legal responsibilities for this.

The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, at least the following precautions shall be implemented by GDCA:

1. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), GDCA shall reject all keys found at https://github.com/cabforum/Debianweak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of Section 6.1.5, with the exception of RSA key sizes greater than 8192 bits, GDCA shall reject Debian weak keys.

2. In the case of ROCA vulnerability, GDCA shall reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.

3. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), GDCA shall reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

6.1.2. 私钥传送给订户 Private Key Delivery to Subscriber

对于由 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 所签发的订户证书，由 GDCA 代替订户提出加密密钥申请请求，GDCA 为订户产生加密密钥对，并使用订户的签名密钥对的公钥进行数字信封加密，以数据流的方式传送给 GDCA，通过 GDCA 下载到订户证书载体时，订户使用签名私钥解密该数字信封，获得加密密钥对并存储在证书载体中。

For the subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, GDCA submits application of an encryption key pair on behalf of the subscribers and generates an encryption key pair for subscriber, and encrypts the key pair using the public key of the subscriber's signing key pair based on the digital envelope technology, and sends it to

GDCA as data stream. The subscriber downloads the digital envelope from GDCA, decrypts it using the private signing key and saves the decrypted encryption key pair in the certificate carrier.

由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的订户证书（安全邮件证书除外）， GDCA 不需要将私钥传递给订户。对于需要传递私钥的安全邮件证书，私钥加密保护后通过安全通道传送给订户，加密及传输的方式符合 S/MIME Baseline Requirements 6.1.2。

For subscriber certificates (S/MIME certificates excepted) issued by Subordinate CAs of GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA certificate and GDCA TrustAUTH E5 ROOT certificate, GDCA does not need to send private keys to subscribers. For the S/MIME certificates that require the delivery of private keys, the private keys shall be delivered encrypted and protected via secure channels to the subscribers, and the method to encrypt and transport private keys conforms to section 6.1.2 of the S/MIME Baseline Requirements.

6.1.3. 公钥传送给证书签发机构 Public Key Delivery to Certificate Issuer

为了获得数字证书，最终订户和 RA 通过 PKCS#10 格式的证书签名请求信息或其它数字签名的文件包格式，以电子的方式将公钥提交给 GDCA 签发，这些请求或文件包的传送需要使用安全协议保护，比如安全套接层协议（SSL）。

In order to obtain a digital certificate, end subscriber and RA sends certification issuance request to GDCA electronically. The request contains public key for GDCA to issue the certificate. The request information is encoded as PKCS#10 or other packing format with digital signature. The transmission of these requests or file packages needs to use security protocol for protection, such as secure sockets layer protocol (SSL).

最终订户和 RA 通过 PKCS#10 格式的证书签名请求信息或其它数字签名的文件包格式，以电子的方式将公钥提交给 GDCA 签发，GDCA 在签发证书前验证所提交请求中的订户签名。

End subscriber and RA sends certification issuance request to GDCA electronically. The request contains public key for GDCA to issue the certificate. The request information is encoded as PKCS#10 or other packing format with digital signature. The subscriber’s signature on the request is authenticated prior to issuing the certificate.

6.1.4. CA 公钥传送给依赖方 CA Public Key Delivery to Relying Parties

GDCA 应该通过安全可靠的途径将 CA 公钥传给依赖方，包括从安全站点下载、面对面的提交等方式。

GDCA shall use secure and reliable way to deliver CA public key to relying party, including download from security site, face to face submission, etc.

GDCA 也需要通过目录发布其 CA 证书。

GDCA also publishes CA certificate through server directory.

6.1.5. 密钥的长度 Key Sizes

对于由 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 所签发的订户证书，GDCA 支持的 RSA 密钥长度为 1024 位或以上，支持的 SM2 密钥长度为 256 位。对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的用户证书，GDCA 支持的 RSA 密钥长度为 2048 位或以上（位数能被 8 整除），支持的 ECC 密钥长度为 256 或以上。如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，GDCA 将会完全遵从。

For the subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, the size of RSA key which GDCA supports is 1024 bits or more, and the size of SM2 key which GDCA supports is 256 bits or more. For the subscriber certificates issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT, 数安时代 R5 根 CA 证书, and GDCA TrustAUTH E5 ROOT, the size of RSA key which GDCA supports is 2048 bits or above (evenly divisible by 8), and the size of ECC key which GDCA supports is 256 bits or above. GDCA will conform to the specifications and requirements of key size from state's laws and regulations, government, etc.

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 GDCA 订户，公钥参数必须使用国家密码主管部门批准许可的加密设备和硬件介质生成，例如加密机、加密卡、USB Key、IC 卡等生成和选取，并遵从这些设备的生成规范和标准。GDCA 认为这些设备和介质内置的协议、算法等已经具备了足够的安全等级要求。

Public key parameters of subscriber who use hardware cryptographic modules must be generated in encryption equipment and hardware medium approved and permitted by OSCCA, such as cryptographic server, cryptographic card, USB Key, IC card, and follow generation standards of these devices. GDCA considers that built-in protocols, algorithms for these devices and medium have already met sufficient level of security requirements.

对于参数质量的检查，同样由通过国家密码主管部门批准许可的加密设备和硬件介质进行，例如加密机、加密卡、USB Key、IC 卡等。

Quality of public key parameters is also checked through the encryption equipment and hardware medium approved and permitted by OSCCA, such as cryptographic server, cryptographic card, USB Key, IC cards. Of course, GDCA considers that built-in protocols, algorithms for these devices and medium have already met sufficient level of security requirements.

6.1.7. 密钥使用目的（基于 X.509 v3 密钥用途字段）Key Usage Purposes (as per X.509 v3 Key Usage Field)

GDCA 签发的 X.509v3 证书包含了密钥用法扩展项，其用法与 RFC 5280 标准(Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008) 相符。如果 GDCA 在其签发证书的密钥用法扩展项内指明了用途，证书订户必须按照该指明的用途使用密钥。

X.509v3certificates issued by GDCA contains key usage extension which meets the RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008).If the key usage is defined in the certificate by GDCA, the certificate subscriber must use the key according to the key usage defined.

参见本 CP 7.1.2。

See CP 7.1.2.

6.2. 私钥保护和密码模块工程控制

Private Key Protection and Cryptographic Module Engineering Controls

认证机构必须通过物理、逻辑和过程控制的综合实现来确保 CA 私钥的安全。订户协议会要求证书订户采取必要的预防措施防止私钥的丢失、泄露、更改或未经授权的使用。

Physical, logical and process control approaches must be synthetically used to ensure the security of CA's private keys. Subscriber agreement will require certificate subscriber to take necessary measures to prevent the loss, leak, changes, or unauthorized use of the private key.

6.2.1. 密码模块的标准和控制 Cryptographic Module Standards and Controls

GDCA 必须使用国家密码管理部门认可、批准的硬件密码模块生成根 CA、签发证书的 CA 和其他 CA 密钥对，并存储相关 CA 私钥。CA 系统的密码模块符合 FIPS 140-2 第三级别的技术要求，订户使用的密码模块符合 FIPS 140-2 第二级别的技术要求。

GDCA must use the Hardware Security Module approved and permitted by OSCCA to generate and store the key pair of root CA, issuing CA and other CAs. The cryptographic module of the CA system meets the FIPS 140-2 Level 3 technical requirements, and the cryptographic modules of the subscribers conform to the FIPS 140-2 level 2 technical requirements.

6.2.2. 私钥多人控制（m 选 n）Private Key (n out of m) Multi-Person Control

认证机构必须通过技术及过程上的控制机制来实现多名可信人员共同参与 CA 加密设备的操作。技术上的控制可使用“秘密分割”技术，即将使用一个 CA 私钥时所需的激活数据分成若干个部分，分别由多名可信人员持有。如果为一个硬件密码模块的秘密分割总数为 m，那么必须有超过 n 个的可信人员才能激活储存在密码模块中的 CA 私钥。在这里 m 不小于 5，n 不小于 3。

CA must use technology and process control mechanisms to achieve multi-reliable personnel jointly participate in the operation of CA encryption equipment. The “Secret Sharing” technology is adopted, namely, the activated data required in operating the private key of CA is split into the several parts and the parts are held by several trusted personnel. If hardware cryptography module’s secret division amount ism, then at least the number of n of trusted personnel must be required to activate CA private key stored in this cryptography module. It notes that m is not less than 5, n is not less than 3.

6.2.3. 私钥托管 Private Key Escrow

不适用。

Not applicable.

6.2.4. 私钥备份 Private Key Backup

为了保证业务持续开展，GDCA 必须创建 CA 私钥的备份，以备灾难恢复使用。私钥备份以加密的形式保存在硬件密码模块中。存储 CA 私钥的密码模块应符合 CP 第 6.2.1 节的要求并存放在保险柜中。CA 私钥复制到备份硬件密码模块中要符合 CP 第 6.2.6 节的要求。

In order to ensure ongoing operations, GDCA must create backup of the CA private key for disaster recovery. Such keys are stored in encrypted form in hardware cryptographic modules and associated key storage devices Backup of the private key in encrypted form is stored in the hardware cryptographic module, and cryptographic modules used for CA private key storage meet the requirements of section 6.2.1 and are stored in safety box. CA private key is copied to backup for hardware cryptographic module to meet the requirements of section 6.2.6.

对于订户签名证书，如果其私钥存放在软件密码模块中，建议订户对私钥进行备份，备份的私钥需要采用口令保护等授权访问控制，防止非授权的修改或泄露。

For subscribers signing certificate, if the private key is stored in the software code module, it is proposed that subscriber’s backup the private key, the backup private key using the password for access control authorized to prevent unauthorized modification or disclosure.

对于订户加密证书，其加密私钥由 GDCA 进行备份，备份私钥以密文形式存在。

For subscriber's encryption certificate, its encryption private key is backed up by GDCA, and backup private key exists in the form of cipher text.

6.2.5. 私钥归档 Private Key Archival

在 CA 私钥到期后，必须使用满足 CP 第 6.2.1 节要求的硬件密码模块归档保存至少 7 年。归档期限结束后，对 CA 私钥的销毁应符合 CP 第 6.2.10 节的规定。

After the expiration of private key, GDCA must use the hardware cryptographic module specified by CP section 6.2.1 to archive and store at least 7 years. After the expiration of archival period, the destruction of private key shall meet the provision of CP section 6.2.10.

6.2.6. 私钥导出、导入密码模块 Private Key Transfer Into or From a Cryptographic Module

CA 的私钥，GDCA 应严格按照根密钥管理规范进行备份，除此之外的任何导入导出操作将不被允许。当 CA 密钥对备份到另外的硬件密码模块上时，以加密的形式在模块之间传送，并且在传递前要进行身份鉴别，以防止 CA 私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

GDCA private key backup is run strictly in accordance with procedure and strategies specified by GDCA, in addition, any data import and export operations are not be allowed. When CA key pair is backed up to another hardware cryptographic module, by the way of the encrypted form to transmit between the modules, and made a authentication before the transmitting to prevent the CA private key from being lost, stolen, modified, disclosure non-authorized, used unauthorized.

GDCA 不提供订户私钥从硬件密码模块中导出的方法，也不允许如此操作。对于存放在软件密码模块中的私钥，如果订户愿意并且自行承担相关风险，订户可自主选择导入导出的方式，操作时需要采用口令保护等授权访问控制措施。

GDCA does not provide the export of subscriber's private key from hardware cryptographic module and allow this operation. As for the private key stored in software cryptographic module, and if subscriber is willing to bear the relevant risks, subscriber can choose the way of import and export with access control such as password, etc.

6.2.7. 私钥在密码模块的存储 Private Key Storage on Cryptographic Module

CA 系统的私钥必须以密文的形式存放在国家密码主管部门批准和许可的硬件密码模块中，硬件密码模块至少符合 FIPS 140-2 三级标准或同等级安全水平。

The private key of CA systems in encrypted form must be stored in Hardware Security Module approved

and permitted by OSCCA, and hardware cryptographic module at least meets the FIPS 140-2 level 3 standards or equivalent security levels.

订户的私钥存储在符合国家密码管理规定的设备或文件证书中，所有在设备中存储的私钥，都以密文的形式保存。对于使用软件密码模块生成的私钥，最好在硬件密码模块中存储和使用，订户也可以自主选择使用有安全保护措施的特定软件密码模块。

Subscriber's private key is stored in the devices or files meeting the regulations of OSCCA. All the private keys stored in the devices are in the form of cipher text. For the private key generated by software cryptographic modules is preferably stored and used in hardware cryptographic modules. Subscriber can also use specific software cryptographic modules with security measures.

用于安全存储代码签名证书订户私钥的硬件密码模块至少符合 FIPS 140-2 二级标准或同等级安全水平。

The hardware cryptographic module used to store the private keys of the code signing certificates at least meets the FIPS 140-2 level 2 standards or equivalent level of security.

6.2.8. 激活私钥的方法 Method of Activating Private Key

CA 的私钥存放于硬件密码模块中，其激活数据按照 CP 第 6.2.2 节进行分割，并且保存在 IC 卡等硬件介质中，必须由 m 选 n 的方式分别输入激活数据才能激活私钥。

The private key of CA shall be saved in hardware cryptographic module, and its activation data shall be spilt in accordance with Section 6.2.2, and be saved in the hardware media such as IC card. The private key must be activated through entering the data using n out of m.

对于存放在诸如 USB Key、加密卡、加密机或者其他形式的硬件密码模块中的订户私钥，订户可以通过口令、IC 卡等方式进一步保护。当订户计算机上安装了相应的驱动后，将 USB Key、IC 卡等插入相应设备中，输入保护口令，则私钥被激活。对于存放在订户计算机软件密码模块中的私钥，订户应该采用合理的措施从物理上保护计算机，以防止在没有得到用户授权的情况下，其他人员使用订户的计算机和相关私钥。如果存放在软件密码模块中的私钥没有口令保护，那么软件密码模块的加载意味着私钥的激活。如果使用口令保护私钥，软件密码模块加载后，还需要输入口令才能激活私钥。

For the private key saved in such as USB Key, cryptographic card, cryptographic server, or other forms of hardware modules, the subscriber can protect through password, IC card, etc. After the appropriate driver is installed in subscriber’s computer, the private key is activated by the way that the USB Key, smart cards are plugged into the appropriate device to enter the protection password. For the private key stored in the subscriber's computer software cryptographic module, the subscriber should take reasonable measures to protect the computers physically in order to prevent unauthorized personnel from using computers and private keys of subscriber. If the private key is stored in software cryptographic module without the password protection, then the loading of software cryptographic module means the activation of private key. The private key protected by password can be activated via inputting password.

6.2.9. 冻结私钥的方法 Method of Deactivating Private Key

一旦私钥被激活，除非这种状态被冻结，私钥总是处于活动状态。在某些私钥的使用当中，私钥每次被激活，只能进行一次操作，如果需要进行第二次操作，需要再次进行激活。

Once the private key is activated, unless the state is deactivated, the private key is always active. In some cases, the private key is activated for one operation and reactivated for another operation.

冻结私钥的方式包括退出登陆状态、切断电源、将硬件密码模块移开、注销用户或系统等。

The ways of deactivating private key include exit, shutdown, removing hardware cryptographic module and logout of user or system. Any unauthorized person can't execute above operation.

对于 CA 私钥，当存放私钥的设备断电，私钥就被冻结。

The private key will be deactivated when its storage device powers off.

订户冻结私钥由其自行决定，当每次操作后注销计算机，或者把硬件密码模块从读卡器中取出，切断电源时，私钥就被冻结。

Subscriber can deactivate the private key by themselves. And private key will be deactivated when logout, or remove hard cryptographic module from card reader, or turn off the power supply.

6.2.10. 解除私钥激活状态的方法 Method of Destroying Private Key

私钥不再使用、不需要保存时，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授权使用。

When private key is no longer used and do not need to be saved, it shall be destroyed so as to avoid loss, stealing and disclosure or unauthorized usage.

对于最终订户加密证书私钥，在其生命周期结束后，应该妥善保存一定期限，以便于解开加密信息。对于最终订户签名证书私钥，在其生命周期结束后，如果无需再保存，由订户决定其销毁方法，可以通过私钥的删除、系统或密码模块的初始化、物理销毁私钥存储模块等方式来销毁。

For end subscriber's encryption certificate private key, after the termination of lifetime, it should be kept certain time so as to decrypt the encrypted information. For end subscriber signature certificate private key, after the termination of lifetime, if it does not need to be kept, subscriber shall determine the method of destroying the private key, including deletion of private key, initialization of system or cryptographic module, physically destroying the private key storage module and other methods.

CA 私钥，在生命周期结束后，需将 CA 私钥的一个或多个备份进行归档，其他的 CA 私钥备份被安全销毁。归档的 CA 私钥在其归档期限结束时需在多名可信人员参与的情况下安

全销毁。CA 私钥存放在硬件加密卡中，CA 私钥的销毁必须通过将 CA 私钥从加密卡中彻底删除或将加密卡初始化的方式销毁。

After the termination of lifetime, GDCA need archive one or more backup of CA private key and securely destroy other CA private key backup. The archived private key of CA shall be destroyed by multiple Trusted Persons during its archiving period. The CA private key is stored in the hardware encryption card, the destruction of CA private key must use the method that the CA private key is deleted from the encryption card completely or is destroyed with encryption card initialization.

6.2.11. 密码模块的评估 Cryptographic Module Rating

GDCA 使用国家密码主管部门批准和许可的密码产品，接受其颁发的各类标准、规范、评估结果、评价证书等各类要求，GDCA 可根据产品性能、工作效率、供应厂商的资质等方面的条件，选择所需要的模块。

GDCA uses the products approved and permitted by OSCCA, and accepts various standards, specifications, assessment, evaluation certification and other requirements published by OSCCA. GDCA could select the module according to product performance, efficiency, supplier qualifications and other aspects.

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

必须归档 CA 和最终订户证书，归档的证书可存放在数据库中。

GDCA must archive CA and end subscriber certificate, and archived certificate can be stored in database.

6.3.2. 证书操作期和密钥对使用期限 Certificate Operational Periods and Key Pair Usage Periods

公钥和私钥的使用期限与证书的有效期相关，但并不完全保持一致。

The usage period of public key and private key is related to the validity period of certificate, but they are not completely consistent.

对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期限以外。

For the signing certificate, its private key can only be used for signing within the certificate validity period

and not be used surpass the validity period of certificate. However, in order to ensure signature information can be verified within the certificate validity period, the public key can be used surpass the validity period of certificate.

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

For the encryption certificate, its public key can only be used for encryption within the validity period of certificate and not be used surpass the validity period of certificate. However, in order to ensure information encrypted can be used to unlock the information within the validity period of certificate, the private key can be used surpass the validity period of certificate.

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

For the certificate used for authentication, the private key and public key can only be used within the validity period of certificate.

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

If a certificate has multiple usages, the usage periods of public key and private key follow the rules described above.

另外需注意的是无论是订户证书还是 CA 证书，证书到期后，在保证安全的情况下，允许使用原密钥对对证书进行更新。但是密钥对不能无限期使用。

In addition, after the expiration of certificate, under the circumstances of ensuring security, original key pair can be used to update the certificate. But the key pair can't be used indefinitely.

对于不同的证书，其密钥对允许通过证书更新的最长使用期限如下：

1. 对 ROOTCA(RSA)签发的 RSA2048 位 CA 证书，其密钥对的最长允许使用年限是 10 年，可少于 10 年；
2. 对 ROOTCA（SM2）签发的 SM2 CA 证书，其密钥对的最长允许使用年限是 20 年，可少于 20 年；
3. 对于 GDCA ROOT CA1 签发的 RSA 2048 位 CA 证书，其密钥对的最长允许使用年限是 13 年，可少于 13 年；
4. 对于 GDCA TrustAUTH E1 CA 签发的 SM2 CA 证书，其密钥对的最长允许使用年限是 12 年，可少于 12 年；
5. 对于 GDCA 的 RSA4096 位根 CA 证书，其密钥对的最长允许使用年限是 30 年，可少于 30 年；
6. 对于 GDCA 的 ECC 384 位根 CA 证书，其密钥对的最长允许使用年限是 30 年，可少于 30 年；
7. 对于 RSA2048 位 SSL/TLS 服务器证书，其密钥对的最长允许使用期限是 398 天，

可少于 398 天；

8. 对于 RSA3072 位代码签名证书，其密钥对的最长允许使用期限是 39 个月，可少于 39 个月；
9. 对于 RSA3072 位时间戳证书，其密钥对的最长允许使用期限是 5 年，可少于 5 年；
10. 对于 RSA2048 位安全邮件证书，其密钥对的最长允许使用期限是 825 天，可少于 825 天；
11. 对于 RSA2048 位除 SSL/TLS 服务器证书及 S/MIME 安全邮件证书外的订户证书，其密钥对的最长允许使用年限是 8 年，可少于 8 年；
12. 对于 SM2 订户证书，其密钥对的最长允许使用年限是 4 年，可少于 4 年；
13. 对于 ECC256 位 SSL/TLS 服务器证书，其密钥对的最长允许使用期限是 398 天，可少于 398 天；
14. 对于 ECC256 位代码签名证书，其密钥对的最长允许使用期限是 39 个月，可少于 39 个月；
15. 对于 ECC256 位除 SSL/TLS 服务器证书及代码签名证书外的订户证书，其密钥对的最长允许使用年限是 8 年，可少于 8 年。

For different certificates, the maximum usage period of the key pair can be obtained via certificate renewal:

1. For ROOTCA (RSA) RSA 2048-bit CA certificate, the maximum usage period of the key pair is 10 years or less than 10 years.
2. For ROOTCA (SM2) SM2 CA certificate, the maximum usage period of the key pair is 20 years or less than 20 years.
3. For GDCA ROOT CA1 RSA 2048-bit CA certificate, the maximum usage period of the key pair is 13 years or less than 13 years.
4. For GDCA TrustAUTH E1 CA SM2 CA certificate, the maximum usage period of the key pair is 12 years or less than 12 years.
5. For the GDCA RSA 4096-bit root CA certificate, the maximum usage period of the key pair is 30 years or less than 30 years.
6. For the GDCA ECC 384-bit root CA certificate, the maximum usage period of the key pair is 30 years or less than 30 years.
7. For the RSA 2048-bit SSL/TLS server certificate, the maximum usage period of the key pair is 398 days or less than 398 days.

8. For the RSA 3072-bit code signing certificate, the maximum usage period of the key pair is 39 months or less than 39 months.
9. For the RSA 3072 bits Timestamp certificate, the maximum usage period of the key pair is 5 years or less than 5 years.
10. For the RSA 2048 bits S/MIME certificate, the maximum usage period of the key pair is 825 days or less than 825 days.
11. For the RSA 2048 bits Subscriber Certificates other than the SSL/TLS server certificates and S/MIME certificates, the maximum usage period of the key pair is 8 years or less than 8 years.
12. For SM2 subscriber certificate, the maximum usage period of the key pair is 4 years or less than 4 years.
13. For the ECC 256 bits SSL/TLS server certificate, the maximum usage period of the key pair is 398 days or less than 398 days.
14. For the ECC 256 bits code signing certificate, the maximum usage period of the key pair is 39 months or less than 39 months
15. For the ECC 256 bits Subscriber certificates beyond the SSL/TLS server certificates and the code signing certificates, the maximum usage period of the key pair is 8 years or less than 8 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

CA 私钥的激活数据，必须按照关于密钥激活数据分割和密钥管理办法的要求，严格进行生成、分发和使用。

Activation data of CA private key must be generated, distributed and used strictly according to the requirements which are related to the segmentation of key activation data and key management.

订户私钥的激活数据，包括用于下载证书的口令（以密码信封的形式提供）、USB Key 的 PIN 码等，都必须在安全可靠的环境下随机产生。

Activation data of subscriber private key, including password (provided in the form of password envelope) used to download the certificate, USB Key, login password of IC card, must be generated randomly in secure and reliable environments.

6.4.2. 激活数据的保护 Activation Data Protection

对于 CA 私钥的激活数据，必须通过秘密分割将分割后的激活数据由不同的可信人员掌管，而且掌管人员必须符合职责分割的要求，签署协议确认他们知悉秘密分割掌管者责任。

Activation data of CA private key must be separated in reliable way and kept by different trusted personnel.

Administrator must meet the requirements of responsibility division. The responsibilities of key sharing holders should be confirmed by signing related agreements.

对于订户私钥的激活数据，包括口令或 PIN 码，都必须在安全可靠的环境下产生。订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。同时为了配合业务系统的安全需求，应该经常对激活数据进行修改。

Subscriber's activation data, including password and PIN, must be generated in the safe and reliable environment. The subscriber should take good care of password or PIN to prevent being exposed or stolen. Meanwhile, in order to meet the security requirements of business systems, activation data should be modified regularly.

6.4.3. 激活数据的其他方面 Other Aspects of Activation Data

当私钥的激活数据进行传送时，应保护它们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

Activation of private key shall be protected from loss, theft, modification, unauthorized disclosure, or unauthorized usage during the transmission.

当私钥的激活数据不需要时应该销毁，并保护它们在此过程中免于丢偷窃、泄露或非授权使用，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或全部，比如记录有口令的纸页必须粉碎。

The activation data of private key which is no longer used shall be destroyed and protected from theft, disclosure or unauthorized use during the destruction. The result of destruction is that some or all of activation data can't be recovered directly or indirectly from the residual information and medium, papers recorded with passwords must be shredded.

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

GDCA 系统的信息安全管理，按照国家密码管理局公布的《信息安全技术 证书认证系统密码及其相关安全技术规范》、工业和信息化部公布的《电子认证服务管理办法》，参照 ISO27001 信息安全标准规范以及其他相关的信息安全标准，制定出全面、完善的安全管理策略和制度，在运营中予以实施、审查和记录。主要的安全技术和控制措施包括：身份识别和验证、逻辑访问控制、物理访问控制、人员职责分权管理、网络访问控制等。

Information security management of GDCA certification system meets "Specifications Related Security

Technology Certificate Authentication System" published by OSCCA, "Information security technology—Specifications of cryptograph and related security technology for certificate authentication system" published by Ministry of Industry and Information Technology, standards of information security in ISO27001 and security standards of other relevant information. GDCA draws up comprehensive and perfect security management strategies and standards, which have been implemented, reviewed and recorded within operation. The main security technologies and control measures include: Identification and authentication, logic access control, physical access control, management of personnel's responsibilities decentralization, network access control, etc.

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。

Strict security controls ensures that the system of CA software and data files is secure and reliable 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。这种分离可以阻止除指定的应用程序外对网络的访问。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。只有 CA 系统操作与管理组中的、有必要工作需要、访问系统的可信人员可以通过口令访问 CA 数据库。

Core system must be separated physically from other systems and the production system must be separated from other system logically. This separation can prohibit network access except for specific applications. The usage of firewall is to prevent the intrusion from the internal and external network production system and restrict activities of access production system. Only trusted persons in operation and management group of CA system, when necessary to access to the system can access the CA database using password.

6.5.2. 计算机安全评估 Computer Security Rating

GDCA 的认证系统，通过了国家密码管理局的安全性审查。

GDCA certification systems pass the security review of OSCCA.

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

GDCA 的软件设计和开发过程遵循以下原则：

1. 第三方验证和审查；
2. 安全风险分析和可靠性设计。

同时，GDCA 的软件开发操作规范，参考 ISO15408 的标准，执行相关的规划和开发控制。

Software design and development of GDCA process follows principles:

1. Verification and review of third-party;
2. The security risk analysis and reliability design.

The operation specifications of software development, which refer to ISO15408 standard, implement relevant plan and development control.

6.6.2. 安全管理控制 Security Management Controls

GDCA 认证系统的信息安全管理，严格遵循国家密码主管部门的有关运行管理规范进行操作。

Information security management of GDCA certification system conforms to the relevant operation management specification of OSCCA strictly.

GDCA 认证系统的使用具有严格的控制措施，所有的系统都经过严格的测试验证后才进行安全和使用，任何修改和升级会记录在案并进行版本控制、功能测试和记录。GDCA 还对认证系统进行定期和不定期的检查和测试。

GDCA authentication system has a strict control measures, and all the systems can be used through rigorous testing and verifying. Any modifications and upgrades will be recorded for reference and made for version control, functional test and record. GDCA also carries out regular and irregular inspection and test for certification system.

GDCA 采用一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。

GDCA uses the flexible management system to control, monitor system configuration and prevent unauthorized modification.

硬件设备由采购到接收时，会进行安全性的检查，用来识别设备是否被入侵，是否存在安全漏洞等。加密设备的采购和安装必须在更加严格的安全控制机制下，进行设备的检验、安装和验收。

Hardware devices are checked from the perspective of intrusion and security holes, etc. Encryption devices must be examined, installed and accepted in a strict security control mechanism.

GDCA 认证系统所有的软硬件设备升级以后，废旧设备在进行处理时，首先必须确认其是否有影响安全的信息存在。

After all the hardware and software equipment of GDCA authentication system are upgraded, GDCA must confirm the existence of information which affects the security in waste equipment.

6.6.3. 生命周期的安全控制 Life Cycle Security Controls

GDCA 认证系统的软硬件设备具备可持续性的升级计划，其中包括了对软、硬件生命周

期的安排。

Software and hardware of GDCA certification system have sustainable upgrade plan such as arrangement of software and hardware lifetimes.

6.7. 网络的安全控制 Network Security Controls

GDCA 认证系统采用多级防火墙和网络资源安全控制系统的保护，并且实施完善的访问控制技术。

GDCA authentication system has multi-level firewalls and the protection of network resource security control systems. It also has complete access control technology.

为了确保网络安全，GDCA 认证系统安装部署了入侵检测、安全审计、防病毒和网管系统，并且及时更新防火墙、入侵检测、安全审计、防病毒和网管系统的版本，以尽可能的降低来自于网络的风险。

GDCA 的网络安全控制须符合 CA/浏览器论坛（CA/Browser Forum）发布的 Network and Certificate System Security Requirements（NCSSR）的要求。

GDCA 至少每季度执行一次网络漏洞扫描，漏洞响应及整改时间表根据漏洞严重程度确定，关键漏洞需在 96 小时内完成响应及整改，高/中危漏洞需在 60 天内响应及整改。对于例外情况，GDCA 应进行记录、风险评估并存档。

In order to ensure network security, GDCA authentication business system has been equipped with intrusion detection, security auditing, virus protection and network management systems, and updated to the version of above systems, as much as possible to reduce the risks from the network.

The network controls adopted by GDCA must conform to the Network and Certificate System Security Requirements (NCSSR) published by the CA/Browser Forum.

Vulnerability scans of networks are performed at least once a quarter by GDCA. Responding and remediation timelines are governed by severity, with critical vulnerabilities addressed within 96 hours and high/medium vulnerabilities resolved within 60 days. Exceptions are documented, assessed for risk, and recorded.

6.8. 时间戳 Time-Stamping

GDCA 提供符合 RFC 3161、5816 以及 Authenticode 的时间戳服务，主要用于代码签名、PDF 签名等用途。GDCA 的业务系统的系统时间均通过 NTP 协议与该时间戳服务同步。

GDCA provides time stamp service that complies with RFC 3161, RFC 5816 and Authenticode, mainly used for code signing and PDF signing purpose, and the system time of GDCA's operation system synchronizes with this time stamp service through Network Time Protocol (NTP).

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. 证书描述 Certificate Profile

GDCA 证书遵循 ITU-T X.509v3（1997）：信息技术-开放系统互连-目录：认证框架（1997 年 6 月）标准和 RFC 5280：Internet X.509 公钥基础设施证书和 CRL 结构（2008 年 5 月）。

The format of GDCA certificates conforms to national standard, i.e. ITU-T X.509 V3 (1997): Information Technology - Open Systems Interconnection - the Directory - Authentication Framework (June 1997) recommendation by ITU-T and RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (May 2008).

GDCA 通过 CSPRNG 生成大于 0 且长度为 64 位的非序列性的证书序列号。

GDCA generates non-sequential certificate serial numbers greater than zero containing 64 bits of output from a CSPRNG.

GDCA 所签发证书结构基本域如下：

域	值或值的限制
版本	指明 X.509 证书的格式版本，值为 V3
序列号	证书的唯一标识符
签名算法	签发证书时所使用的签名算法（见 CP 第 7.1.3 节）
签发者 DN	签发者的甄别名
有效起始日期	基于国际通用时间(UTC)，和北京时间同步，按 RFC 5280 要求编码
有效终止日期	基于国际通用时间(UTC)，和北京时间同步，按 RFC 5280 要求编码。有效期限的设置符合 CP 第 6.3.2 节规定的限制。
主题 DN	证书持有者或实体的甄别名如下： CA 根证书 DN：CN、O、C。 中级 CA 证书 DN：CN、O、C。 订户机构证书 DN：CN、O、OU（可选）、L、S、C。 订户机构个人证书 DN：CN、O、OU（可选）、L、S、C。 订户设备证书 DN：CN、O、OU（可选）、L、S、C。 订户基础邮件证书 DN：E、CN。

	订户个人邮件证书 DN：E、CN、L、S、C。 订户机构邮件证书 DN：E、CN、O、organizationIdentifier、OU（可选）、L、S、C。 订户机构个人邮件证书 DN：E、CN、O、organizationIdentifier、OU（可选）、L、S、C。 订户个人证书 DN：CN、L、S、C。 订户 DV SSL 证书 DN：CN。 订户 OV SSL 证书 DN：CN、O、L、S、C。 订户 EV SSL 证书 DN：CN、O、streetAddress（可选）、postalCode（可选）、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）。 订户 EV 代码签名证书 DN：CN、O、streetAddress（可选）、postalCode（可选）、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）
公钥	根据 RFC 5280 编码，使用 CP 第 7.1.3 节中指定的算法，密钥长度满足 CP 第 6.1.5 节指定的要求

Following are the basic certificate fields for the certificates issued by GDCA:

Fields	Value or value limitation
Version	Format version of X.509 certificate with the value is V3
Serial number	Unique identifier of certificate
Signature algorithm	Signature algorithm for issuing certificate（see CP section 7.1.3）
Issuer	Issuer's Distinguish Name
notBefore	Based on the Coordinated Universal Time (UTC), Synchronized with Beijing time, encoding follows the requirements of RFC 5280.
notAfter	Based on the Coordinated Universal Time (UTC), Synchronized with Beijing time, encoding follows the requirements of RFC 5280. The setting of valid period follows the limitation of this CP Section 6.3.2 specified.
Subject	Subject DN of a certificate holder or entity may be as follows:

	DN of a root CA certificate: CN, O, C. DN of a subordinate CA certificate: CN, O, C. DN of a subscriber organization certificate: CN, O, OU (Optional), L, S, C. DN of a subscriber individual certificate: CN, O, OU (Optional), L, S, C. DN of a subscriber organization employee certificate: CN, O, OU (Optional), L, S, C. DN of a subscriber equipment certificate: CN, O, OU, L, S, C. DN of a subscriber Basic S/MIME certificate: E, CN. DN of a subscriber IV S/MIME certificate: E, CN, L, S, C. DN of a subscriber OV S/MIME certificate: E, CN, O, organizationIdentifier, OU (Optional), L, S, C. DN of a subscriber SV S/MIME certificate: E, CN, O, organizationIdentifier, OU (Optional), L, S, C. DN of a subscriber individual certificate: CN, L, S, C. DN of a subscriber DV SSL certificate: CN. DN of a subscriber OV SSL certificate: CN, O, L, S, C. DN of a subscriber EV SSL certificate：CN, O, streetAddress (Optional), postalCode (Optional), 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）. DN of a subscriber EV codesigning certificate: CN, O, streetAddress (Optional), postalCode (Optional), 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）
Public key	Using specified algorithm of CP Section 7.1.3 according to the encode of RFC 5280，key length meets specified requirements of CP Section 6.1.5.

7.1.1. 版本号 Version Number(s)

GDCA 订户证书符合 X.509 V3 证书格式，版本信息存放在证书版本信息栏内。

GDCA certificates are in line with X.509 V3 certificate format. The version information is stored in the field of the certificate version column.

7.1.2. 证书扩展项 Certificate Extensions

GDCA 除了使用 X.509 V3 版证书标准扩展项以外，还使用了自定义扩展项。

In addition to the X.509 V3certificate standard extensions, GDCA also uses custom extensions.

7.1.2.1. 根证书 Root CA Certificate

1. 基本约束

根证书须设置该扩展项，且该扩展项为关键扩展项，主体类型被设为 CA，“pathLenConstraint”字段未设置。

2. 密钥用法

根证书须设置该扩展项，且该扩展项关键扩展项，用法设置为 KeyCertSign，CRLSign。根证书对应的私钥不用于签署 OCSP 响应。

3. 证书策略

该扩展项未设置。

4. 增强型密钥用法

该扩展项未设置。

5. 主题密钥标识符

根证书须设置该扩展项，且该扩展项不应标记为关键扩展项，它的值应该包含在根证书签发的证书中的 authorityKeyIdentifier 扩展的 keyIdentifier 字段中。

1. basicConstraints

This extension shall appear and shall be marked critical. The cA field shall be set true, and the pathLenConstraint field is not present.

2. keyUsage

This extension shall be present and shall be marked critical. The usage keyCertSign and cRLSign shall be set. The private key corresponding to a Root CA will not be used for signing OCSP responses.

3. certificatePolicies

This extension is not set for root CA certificates.

4. extKeyUsage

This extension is not set for root CA certificates.

5. subjectKeyIdentifier

This extension shall be present and shall not be marked critical. It shall contain a value that is included in the keyIdentifier field of the authorityKeyIdentifier extension in certificates issued by the Root CA.

7.1.2.2. 中级 CA 证书 Subordinate CA Certificate

1. 证书策略

中级 CA 证书中须设置该扩展项，且不得为关键扩展项，有关具体的策略标识符的信息请见本 CP 的第 1.4.1.8。

2. CRL 分发点

中级 CA 证书中须设置该扩展项，且不得为关键扩展项，该扩展项须包含 CA CRL 服务的 HTTP 地址。

3. 颁发机构信息访问

对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 证书，中级 CA 证书应设有颁发机构信息访问扩展项，且不得为关键扩展项。此扩展中会包含指向此 CA 证书签发者证书的 HTTP 地址（AccessMethod=1.3.6.1.5.5.7.48.2）和指向 CA OCSP 服务的 HTTP 地址（AccessMethod=1.3.6.1.5.7.48.1）。

对于由 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 证书，中级 CA 证书可设有颁发机构信息访问扩展项，若设置，则不得为关键扩展项，此扩展中会包含指向此 CA 证书签发者证书的 HTTP 地址（AccessMethod=1.3.6.1.5.5.7.48.2）和指向 CA OCSP 服务的 HTTP 地址（AccessMethod=1.3.6.1.5.5.7.48.1）。

4. 基本约束

中级 CA 证书须设置该扩展项，且该扩展项为关键扩展项，主体类型被设为 CA，“pathLenConstraint”字段可设置。

5. 密钥用法

中级 CA 证书中须设置该扩展项，且为关键扩展项，且必须设置 KeyCertSign，CRLSign 用法。中级 CA 证书对应的私钥不用于签署 OCSP 响应。

6. 增强型密钥用法

对于在 2019 年 1 月 1 日后由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 证书，中级 CA 证书中须设置该扩展项，且不应为关键扩展项，若该类中级 CA 证书将被用于签发 SSL/TLS 证书，则该扩展项须含 id-kp-serverAuth 【RFC5280】，可包含 id-kp-clientAuth 【RFC5280】，不得包含 id-kpemailProtection 【RFC5280】，id-kp-codeSigning 【RFC5280】，id-kptimeStamping

【RFC5280】，id-kp-OCSPSigning 【RFC5280】及 anyExtendedKeyUsage 【RFC5280】，也不得包含任何其他值。

7. 颁发机构密钥标识符

中级 CA 证书须设置该扩展项，且不得为关键扩展项。该扩展项仅包含 KeyIdentifier 字段。

8. 主题密钥标识符

中级 CA 证书须设置该扩展项，且该扩展项不应标记为关键扩展项，它的值应该包含在中级 CA 签发的证书中的 authorityKeyIdentifier 扩展的 keyIdentifier 字段中。

1. certificatePolicies

This extension for subordinate CA certificates shall be present and shall not be marked critical. More information about the asserted OIDs is explained in section 1.4.1.8 of this CP.

2. cRLDistributionPoints

This extension for subordinate CA certificates shall be present and shall not be marked critical. It shall contain the HTTP URL of the CA's CRL service.

3. authorityInformationAccess

For subordinate CAs issued by GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA 证书 and GDCA TrustAUTH E5 ROOT, this extension should be present and shall not be marked critical. It should contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). It may contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

For the subordinate CAs issued by ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, this extension may be present, and shall not be marked critical if present. It should contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). It may contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

4. basicConstraints

This extension for subordinate CA certificates shall be present and shall be marked critical. The cA field shall be set true. The pathLenConstraint field may be present.

5. keyUsage

The subordinate CA certificates have the "keyUsage" extension, which is a critical extension. Usage settings are: digitalSignature, keyCertSign, cRLSign. The private key corresponding to a subordinate CA certificate will not be used for signing OCSP responses.

6. extKeyUsage

For subordinate CAs issued by GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA 证书 and GDCA TrustAUTH E5 ROOT after 1 January 2019, this extension shall be present and should not be

marked critical. If such subordinate CA certificates will be used to issue SSL/TLS certificates, the value id-kp-serverAuth [RFC5280] shall be present. The value id-kp-clientAuth [RFC5280] may be present. The values id-kpemailProtection [RFC5280], id-kp-codeSigning [RFC5280], id-kptimeStamping [RFC5280], id-kp-OCSPSigning [RFC5280] and anyExtendedKeyUsage [RFC5280] shall not be present. Other values should not be present.

7. authorityKeyIdentifier

This extension for subordinate CA certificates shall be present and shall not be marked critical. This extension contains only the "KeyIdentifier" field.

8. subjectKeyIdentifier

This extension shall be present and shall not be marked critical. It shall contain a value that is included in the keyIdentifier field of the authorityKeyIdentifier extension in certificates issued by the subordinate CA.

7.1.2.3. 订户证书 Subscriber Certificate

1. 证书策略

订户证书中须设置该扩展项，且不得为关键扩展项，有关具体的策略标识符的信息请见本 CP 的第 1.4.1.8 节。

2. CRL 分发点

对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的订户证书，该类订户证书须设置该扩展项项，且此扩展项为非关键扩展。此扩展项中会包含指向 CA CRL 服务的 HTTP URL 地址。

对于由 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 所签发的用户证书，该类订户证书可设置该扩展项项，若设置，则该扩展项为非关键扩展。此扩展项中会包含指向 CA CRL 服务的 HTTP URL 地址。

3. 颁发机构信息访问

对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的订户证书，订户证书须设有颁发机构信息访问扩展项，且不得为关键扩展项。此扩展中会包含指向此 CA 证书签发者证书的 HTTP 地址（AccessMethod=1.3.6.1.5.5.7.48.2）和指向 CA OCSP 服务的 HTTP 地址（AccessMethod=1.3.6.1.5.5.7.48.1）。

对于由 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 所签发的订户证书，该类订户证书可设有颁发机构信息访问扩展项，若设置，则不得为关键扩展项，此扩展中会包含指向此 CA 证书签发者证书的 HTTP 地址

（AccessMethod=1.3.6.1.5.5.7.48.2）和指向 CA OCSP 服务的 HTTP 地址（AccessMethod=1.3.6.1.5.5.7.48.1）。

4. 基本约束

对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的 SSL/TLS 订户证书，可设置该扩展项，若设置，则该扩展项须为关键扩展项，此扩展中“cA”字段须设置为“False”。

对于由 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 所签发的订户证书，可设置该扩展项，若设置，则此扩展中“cA”字段须设置为“False”。

5. 密钥用法

订户证书可设置该扩展项，若设置，则密钥用法不得设置为 keyCertSign 及 cRLSign。

6. 增强型密钥用法

对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的用户证书，证书中的密钥用法及增强型密钥用法如下：

证书类别	密钥用法	备注
邮件证书（原个人 1 类证书）	密钥用法：数字签名，密钥加密，数据加密。 增强型密钥用法：客户端身份验证，电子邮件保护。	2022 年 11 月 1 日起不再用于安全邮件证书。
Adobe 文档签名证书	密钥用法：数字签名，不可否认； 增强型密钥用法：Adobe 文档签名。	
机构个人邮件证书	密钥用法：数字签名，密钥加密，数据加密。 增强型密钥用法：客户端身份验证，电子邮件保护。	
机构邮件证书	密钥用法：数字签名，密钥加密，数据加密。 增强型密钥用法：客户端身份验证，电子邮件保护。	
个人邮件证书	密钥用法：数字签名，密钥加密，数据加密。 增强型密钥用法：客户端身份验证，电子邮件保护。	
基础邮件证书	密钥用法：数字签名，密钥加密，数据加密。 增强型密钥用法：客户端身份验证，电子邮件保护。	
DV SSL 证书	密钥用法：数字签名， 密钥加密。	

	增强型密钥用法：客户端身份验证 ，服务器身份验证。	
OV SSL 证书	密钥用法：数字签名， 密钥加密。 增强型密钥用法：客户端身份验证 ，服务器身份验证。	
IV SSL 证书	密钥用法：数字签名， 密钥加密。 增强型密钥用法：客户端身份验证 ，服务器身份验证。	
EV SSL 证书	密钥用法：数字签名， 密钥加密。 增强型密钥用法：客户端身份验证 ，服务器身份验证。	
普通代码签名类证书	密钥用法：数字签名。 增强型密钥用法：代码签名。	
EV 代码签名证书	密钥用法：数字签名。 增强型密钥用法：代码签名。	
时间戳证书	密钥用法：数字签名。 增强型密钥用法：时间戳。	

7. 颁发机构密钥标识符

订户证书须设置该扩展项，且不得为关键扩展项。该扩展项仅包含 KeyIdentifier 字段。

8. 主题密钥标识符

订户证书须设置该扩展项，且该扩展项不应标记为关键扩展项，它应该包含一个从订户证书中的公钥派生出来的值。

1. certificatePolicies

This extension for subscriber certificates shall be present and shall not be marked critical. More information about the asserted OIDs is explained in section 1.4.1.8 of this CP.

2. cRLDistributionPoints

For the subscriber certificates issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT, 数安时代 R5 根 CA 证书, and GDCA TrustAUTH E5 ROOT, this extension shall be present and shall not be marked critical. It shall contain the HTTP URL of the CA's CRL service.

For the subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, this extension may be present and shall not be marked critical if present. It shall contain the HTTP URL of the CA's CRL service.

3. authorityInformationAccess

For the subscriber certificates issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA 证书 and GDCA TrustAUTH E5 ROOT, this extension shall be present and shall not be marked critical. This extension will contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) and the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

For the subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, this extension may be present, and shall not be marked critical if present. This extension will contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) and the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

4. basicConstraints

For the SSL/TLS subscriber certificates issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA 证书 and GDCA TrustAUTH E5 ROOT, this extension may be present and shall be marked critical if present, and the cA field shall be set to "False" if present.

For the subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, this extension may be present, and the cA field shall be set to "False" if present.

5. keyUsage

This extension for subscriber certificates may be present, and if present, usage keyCertSign and cRLSign shall not be set.

6. extKeyUsage

For the subscriber certificates issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA 证书 and GDCA TrustAUTH E5 ROOT, key usage and extended key usage are as follows:

Types of Certificates	**Key Usages**	**Remarks**
Email Certificates (Previously the Type I Individual Certificates)	KU: Digital Signature, Key Encipherment. EKU: Client Authentication, Email Protection.	This policy OID will not be used to identify the email certificates as of 1 November 2022.
Adobe PDF Signing Certificates	KU: Digital Signature, Non Repudiation. EKU: Adobe Document Signing.	
SV S/MIME Certificates	KU: Digital Signature, Key Encipherment, Data Encipherment. EKU: Client Authentication, Email Protection.	
OV S/MIME Certificates	KU: Digital Signature, Key Encipherment, Data Encipherment.	

	EKU: Client Authentication, Email Protection.	
IV S/MIME Certificates	KU: Digital Signature, Key Encipherment, Data Encipherment. EKU: Client Authentication, Email Protection.	
Basic S/MIME Certificates	KU: Digital Signature, Key Encipherment, Data Encipherment. EKU: Client Authentication, Email Protection.	
DV SSL Certificates	KU: Digital Signature, Key Encipherment. EKU: Client Authentication, Server Authentication.	
OV SSL Certificates	KU: Digital Signature, Key Encipherment. EKU: Client Authentication, Server Authentication.	
IV SSL Certificates	KU: Digital Signature, Key Encipherment. EKU: Client Authentication, Server Authentication.	
EV SSL Certificates	KU: Digital Signature, Key Encipherment. EKU: Client Authentication, Server Authentication.	
Standard Code Signing Certificates	KU: Digital Signature. EKU: Code Signing.	
EV Code Signing Certificates	KU: Digital Signature. EKU: Code Signing.	
TimeStamp Certificates	KU: Digital Signature. EKU: Time Stamping.	

7. authorityKeyIdentifier

This extension for subscriber certificates shall be present and shall not be marked critical. This extension contains only the "KeyIdentifier" field.

8. subjectKeyIdentifier

This extension shall be present and shall not be marked critical. It shall contain a value that is included in the keyIdentifier field of the authorityKeyIdentifier extension in certificates issued by the subordinate CA.

7.1.2.4. 所有证书 All Certificates

GDCA 签发的所有证书均符合 RFC5280，对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 证书，以及中级 CA 证书签发的订户证书，密钥用法、增强型密钥用法及证书扩展项均符合本 CP 第 7.1.2.1、7.1.2.2、及 7.1.2.3 的要求。

对于由 ROOTCA（RSA）证书、GDCA ROOT CA 证书、ROOTCA (SM2)、GDCA ROOT CA1 证书签发的中级 CA 证书，以及中级 CA 证书签发的订户证书，GDCA 除了使用 RFC5280 定义的标准项和标准扩展项以外，还可使用自定义扩展项，例如，针对不同的证书应用服务需求，GDCA 可灵活定义一些扩展项，包括但不限于如下扩展项：

1. 统一社会信任代码号：用于表示企业统一社会信任代码。
2. 信任服务号：证书颁发机构产生用于标识订户的唯一编号。
3. 个人身份证号码：用于表示居民身份证的唯一编号。

For the subscriber certificates and the subordinate CA certificates that chain up to GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA 证书 and GDCA TrustAUTH E5 ROOT, key usages, extended key usages and certificate extensions conform to section 7.1.2.1, 7.1.2.2, and 7.1.2.3 of this CP.

For the subscriber certificates and the subordinate CA certificates that chain up to ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, in addition to the standard fields and extensions defined by RFC 5280, GDCA may also use customized extensions, for example, to satisfy different requirements for certificate application services, GDCA may define some extensions flexibly, including but not limited to the following extensions:

1. Unified social credit identifier: It is used to indicate the unified social credit identifier.

2. Trusted service number: It is used to indicate subscriber’s unique number generated by GDCA.

3. Resident identity card number: It is used to indicate unique number of resident’s identity card.

7.1.2.5. RFC5280 的应用 Application of RFC 5280

为澄清起见，RFC 6962 定义的“预证书”不被视为 RFC5280 定义的“证书”。

For purposes of clarification, a precertificate, as described in RFC 6962 shall not be considered to be a "certificate" subject to the requirements of RFC 5280.

7.1.3. 算法对象标识符 Algorithm Object Identifiers

GDCA 签发的数字证书使用以下相关算法之一：

Sha1RSA withRSAEncryption	1.2.840.113549.1.1.5
sha256RSA withRSAEncryption	1.2.840.113549.1.1.11
SHA256 with ECDSA	1.2.840.10045.4.3.2
SM3withSM2Encryption	1.2.156.10197.1.501

由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 证书签发的公开可信任证书及 OCSP 证书的密码算法不使用 sha1RSA。

GDCA uses one of the following relevant algorithms to issue certificates:

Sha1RSA withRSAEncryption	1.2.840.113549.1.1.5
sha256RSA withRSAEncryption	1.2.840.113549.1.1.11
SHA256 with ECDSA	1.2.840.10045.4.3.2
SM3withSM2Encryption	1.2.156.10197.1.501

Subscriber certificates and OCSP certificates that chain up to the subordinate CA certificates issued by GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA 证书 and GDCA TrustAUTH E5 ROOT are not signed with sha-1WithRSAEncryption.

7.1.4. 名称形式 Name Forms

GDCA 签发的证书名称形式的格式和内容符合 X.501 Distinguished Name(DN)的甄别名格式。

对于由 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 签发的中级 CA 所签发的订户证书，其名称形式的格式和内容格式符合 RFC5280，及 CA/B 论坛发布的 Baseline Requirements 以及 S/MIME Baseline Requirements 7.1.4 节的要求。

GDCA 根据本 CP 的要求签发证书，确保证书签发时，证书主题中的信息都是准确的。GDCA 不会将域名和 IP 地址写入证书主题属性中除非遵循本 CP 第 3.2.9 节和第 3.2.12 节的

规定。

SSL/TLS 证书主题项不能仅含有诸如“.”，“-”，及“ ”（空格）字符，及/或其他任何表示该项为空、不完整、或不适用的内容。

Name of certificate issued by GDCA is formatted in accordance with X.501 DN. For subscriber certificates issued by the subordinate CAs that are issued by GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA 证书 and GDCA TrustAUTH E5 ROOT, the format and content of the name forms of these certificates match the requirements as defined in RFC5280, and CA/Browser Forum Baseline Requirements and S/MIME Baseline Requirements Section 7.1.4.

GDCA issues certificates in accordance with this CP and shall make sure that the information in the certificate subject field are correct. GDCA will not write domain names or IP address into a certificate subject unless they have been strictly validated according to section 3.2.9 and 3.2.12 of this CP.

SSL/TLS server certificates cannot only contain metadata such as '.', '-' and ' ' (empty) characters and/or any other indication that the value/field is absent, incomplete, or not applicable.

7.1.5. 名称限制 Name Constraints

GDCA 可根据 RFC5280 来使用名称限制扩展项，以限制中级 CA 证书的业务应用范围。

GDCA may use the name constraints extension per RFC 5280, in order to limit the business scope of subordinate CA certificates.

7.1.6. 证书策略对象标识符 Certificate Policy Object Identifier

当使用证书策略扩展项时，证书中包含证书策略的对象标识符，该对象标识符与相应的证书类别对应。

When the certificate policy extension is used, the certificate contains object identifier of CP, and the object identifier is in accordance with the corresponding certificate category.

7.1.7. 策略限制扩展项的用法 Usage of Policy Constraints Extension

不适用。

Not applicable.

7.1.8. 策略限定符的语法和语义 Policy Qualifiers Syntax and Semantics

不适用。

Not applicable.

7.1.9. 关键证书策略扩展项的处理语义 Processing Semantics for the Critical Certificate Policies Extension

不适用。

Not applicable.

7.2. 证书撤销列表 CRL Profile

GDCA 定期签发 CRL，供用户查询使用。

依本 CP 签发的 CRL 符合 RFC5280 标准。CRL 至少包含如下表所述基本域和内容。

The CRL determined in this CP is accordance with RFC5280. CRL contains at least basic domain and content described in the following table:

域	值或者值的限制
版本	V2
颁发者	签发 CRL 的实体，颁发者甄别。
生效日期	CRL 的签发日期
下次更新	CRL 下次签发的日期。CRL 每隔 24 小时更新
签名算法	签发 CRL 所使用的签名算法
颁发机构密钥标识符	由 160 位的颁发证书机构公钥进行散列运算后的值构成
撤销列表	列出撤销的证书，包括撤销证书的序列号和撤销日期

Domain	Value or value limitation
Version	V2
Issuer	Entity for issuing CRL, issuer distinguish.
This update	Issuance date of CRL.
Next update	Next issuance date of CRL. CRL is updated every 24 hours.
Signature	signature algorithm used for issuing CRL.
Authority key identifier	It's composed of a 160-bit hash of the value of CA's public key.
Revoked Certificates	List of the revoked certificates, including serial number and revocation date of revocation certificate.

7.2.1. 版本 Version Number(s)

GDCA 目前签发 X.509 V2 版本的 CRL，此版本号存放在 CRL 版本格式栏目中。

GDCA currently issues CRL of X.509 V2 version. This version number is stored in format column of CRL.

7.2.2. CRL 和 CRL 条目扩展项 CRL and CRL Entry Extensions

GDCA 签发符合 RFC5280 的 CRL 和 CRL 扩展项。

关于理由码，若设置该项，则该 CRL 条目扩展项不得为关键扩展项。对于具备 SSL/TLS 证书签发技术能力的 CA，若 CRL 条目是针对根 CA 或中级 CA 证书的，则必须设置该 CRL 条目扩展项。对于不具备 SSL/TLS 证书签发技术能力的 CA，则可基于以下情况设置或省略该 CRL 条目扩展项：CRLReason 值不可为 unspecified (0)。若撤销理由未明确，则 GDCA 必须省略 reasonCode 条目扩展项（须符合上述要求）。若 CRL 条目是针对 SSL/TLS 订户证书，则 CRLReason 值不可为 certificateHold (6)。

若设置了 reasonCode 扩展项，则 CRLReason 值必须为 RFC5280 以及本 CP 第 4.9.1 中最相关的理由。

GDCA issues CRLs with entry extensions in accordance with RFC 5280.

With regard to reason code: If present, this CRL entry extension shall not be marked critical. For CAs technically capable of issuing SSL/TLS certificates, if a CRL entry is for a Root CA or subordinate CA certificate, this CRL entry extension shall be present. If a CRL entry is for a CA not technically capable of causing issuance, this CRL entry extension may be present or omitted, subject to the following requirements: The CRLReason indicated shall not be unspecified (0). If the reason for revocation is unspecified, issuing CAs shall omit reasonCode entry extension, if allowed by the previous requirements. If a CRL entry is for a SSL/TLS certificate, the CRLReason shall not be certificateHold (6).

If a reasonCode CRL entry extension is present, the CRLReason shall indicate the most appropriate reason for revocation of the certificate based on RFC 5280 and section 4.9.1 of this CP.

7.3. OCSP 描述 OCSP Profile

GDCA 为用户提供 OCSP（在线证书状态查询服务），OCSP 作为 CRL 的有效补充，方便证书用户及时查询证书状态信息。GDCA 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，RFC6960），该协议定义了一种标准的请求和响应信息格式以确认证书是否被撤销了。

As an effective supplement of CRL, OCSP provided by GDCA is used to check the information of certificate status for subscriber online. GDCA adopts an Online Certificate Status Protocol (OCSP, RFC6960) developed by IETF PKIX working group. This protocol defines a standard request and response information formats to query whether a certificate is revoked.

若 OCSP 响应服务是为根证书或中级 CA 证书提供，且该类证书已被撤销，则在 CertStatus 的 RevokedInfo 中，revocationReason 字段必须设置。

CRLReason 必须为本 CP 第 7.2.2 章中允许的理由码。

If an OCSP response is for a root CA or subordinate CA Certificate, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus shall be present.

The CRLReason indicated shall contain a value permitted for CRLs, as specified in section 7.2.2 of this CP.

7.3.1. 版本号 Version Number(s)

RFC6960 定义的 OCSP 版本。

The field conforms to OCSP defined in RFC6960.

7.3.2. OCSP 扩展项 OCSP Extensions

不适用。对于 SSL/TLS 证书，OCSP 响应的 singleExtension 不可包含 CRL 条目的 reasonCode 扩展项。

Not applicable. The singleExtension of an OCSP response cannot contain the reasonCode CRL entry extension for SSL/TLS certificates.

8. 认证机构审计和其他评估 Compliance Audit and Other Assessments

8.1. 评估的频度或情形 Frequency or Circumstances of Assessment

GDCA 应每季度内部进行一次一致性审计和运营评估，并每次抽取至少 3%数量的证书进行评估，以保证证书服务的可靠性、安全性和可控性。所抽取的证书为 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 证书签发的中级 CA 所签发的 SSL/TLS 服务器证书。

GDCA shall conduct a compliance audit and an operation assessment each quarter to ensure the reliability, security and controllability of certification services. We extract at least 3% of certificates for assessment. The extracted certificates are SSL/TLS server certificates issued by subordinate CA of TrustAUTH R5 ROOT certificate and 数安时代 R5 根 CA certificate and GDCA E5 ROOT certificate.

除了内部审计和评估外，GDCA 还聘请独立的审计师事务所，按照 WebTrust 对 CA 的规则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》等的要求，每年一次接受主管部门的评估和检查。
2. GDCA 按照国家主管部门的要求、国家相关标准和本 CP 的规定实施运营和服务，按照内部评估和审计规范，每年至少定期执行一次内部的评估审核，包括对 GDCA 内其它实体（RA、受理点等）的评估审核。
3. GDCA 聘请独立的审计师事务所，按照 WebTrust 对 CA 的审计规则，每年进行一次外部审计和评估。
4. GDCA 每年进行一次风险评估工作，识别内部与外部的威胁，并评估威胁事件发生的可能性及造成的损害，并评估目前的应对策略、技术、系统以及相关措施是否足够应对风险，根据风险评估，创建、实施并维持涵盖安全流程、措施及产品的安全计划。

In addition to internal audits and assessments, GDCA also engages external audit firms to perform assessments and evaluations according to the requirements of WebTrust on CA.

1. GDCA is assessed and inspected once a year in accordance with the "Electronic Signature Law of the People's Republic of China", "Measures for the Administration of Electronic Certification Services" and other requirements by administrative authorities.
2. GDCA conducts operations and services according to the requirements of state’s authorities, the specifications of state’s relevant standards and this CP. GDCA shall conduct internal assessment and audit to other entities (including RA or LRA, etc.) in GDCA at least once a year.
3. GDCA engages external audit firms to conduct assessments and evaluations once a year to be compliant with WebTrust for CA.
4. GDCA performs a risk assessment once a year to identify internal and external threats, and to evaluate the possibility of occurrence and potential damages, and to assess if the current strategies, technologies, systems and relevant measures are able to mitigate these risks. Based on the risk assessment, GDCA develops, implements, and maintains a security plan consisting of security procedures, measures, and products.

8.2. 评估者的身份/资格 Identity/Qualifications of Assessor

GDCA 的内部审计，由 GDCA 安全策略委员会负责组织跨部门的审计评估小组，由审计评估小组执行此项工作。

GDCA 聘请的外部审计机构，应该具备以下的资质：

1. 必须是经许可的、有执业资格的评估机构，在业界享有良好的声誉
2. 了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和操作
3. 具备检查系统运行性能的专业技术和工具

4. 具备独立审计的精神

Cross department audit assessment group organized by GDCA Security Policy Committee performs internal audit of GDCA.

External auditors which GDCA hires shall have the following qualifications:

1. Must be an authority which has been licensed and has a good reputation.
2. Understand computer information security system, communication network security requirements, PKI technology, and related standards and operations.
3. Have the expertise and tools to check the system operation and functionality.
4. Be independent.

8.3. 评估者与被评估者之间的关系

Assessor's Relationship to Assessed Entity

1. GDCA 审计员与本机构的系统管理员、业务管理员、业务操作员的工作岗位不能重叠。
2. 外部评估者(信息产业主管部门、独立审计师事务所以及其他机构)和 GDCA 之间是独立的关系，没有任何的业务、财务往来，或者其它任何利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对 GDCA 进行评估。

1. Segregation of duties is required between the GDCA auditors, and the GDCA system administrators, business administrators, and business operators.
2. The external evaluators (information industry department, independent audit firms and other authorities) and GDCA are independent from each other. There is no business inter actions, financial transactions, or any other interests that could affect the objectivity of the assessment between the above two. Assessors should evaluate GDCA in an independent, fair and unbiased attitude.

8.4. 评估的内容 Topics Covered by Assessment

GDCA 内部审计的内容包括：

GDCA's internal audit includes:

1. 安全策略是否得到充分的实施；
2. 运营工作流程和制度是否得到严格遵守；
3. 是否严格按 CP、业务规范和安全要求开展认证业务；
4. 各种日志、记录是否完整，是否存在问题；

5. 是否存在其他可能存在的安全风险。

第三方审计师事务所按照 WebTrust For CA 规范的要求，对 GDCA 进行独立审计。

1. Whether the security strategy is fully implemented
2. Whether operation procedures and processes strictly followed
3. Whether strictly following the CP, business specifications and security requirements when conducting authentication services
4. Whether all kinds of logs and records are preserved and if there is any question
5. If there's any other potential security risks

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

8.5. 对问题与不足采取的行动 Actions Taken as a Result of Deficiency

对于 GDCA 内部审计结果中的问题，由审计评估小组负责监督这些问题的责任职能部门进行业务改进和完善的情况。完成对审计结果的改进后，各职能部门必须向审计评估小组提交业务改进工作总结报告。

Audit assessment group monitors responsible departments for improvements and complete status of issues that were mentioned in audit reports. After improvement of audit results have completed, various functional departments should submit summary of improvement to audit assessment group.

对于 GDCA 授权注册机构的审计结果，如该机构正在进行违反本 CP 及 GDCA 制定的其他业务规范的行为，GDCA 将予以制止，并有权责令其立即停止这些行为，同时根据 GDCA 的要求进行业务整改。业务违规行为情节严重的注册机构，GDCA 将终止对该机构的电子认证业务有关授权。

For authorized RA mentioned in GDCA's audit report, if they are violating the CP and other business standards defined by GDCA, GDCA will stop the above behaviors immediately and ask them to make changes in accordance with the requirements of GDCA. GDCA will terminate relevant authorization of electronic certification services of RA if the above behaviors are seriously violated.

第三方审计师事务所评估完成后，GDCA 按照其工作报告进行整改，并接受再次审计和评估。

If assessments of a third-party auditor firm are completed, GDCA will rectify in accordance with the audit reports. GDCA will be evaluated again after the rectification.

8.6. 评估结果的传达与发布 Communications of Results

GDCA 的内部审计结果应向本机构各职能部门以及审计涉及的注册机构进行正式通报，对可能造成订户安全隐患，GDCA 必须及时向订户通报。

Audit results are formally informed to relevant departments of GDCA and related RA. GDCA will notify the subscribers of any potential security risks timely.

第三方审计师事务所评估完成后，对于审计的结果，将通过 www.gdca.com.cn 网站进行公布。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 GDCA 表明通知的目的和方式，并征得 GDCA 的同意，法律另有规定的除外；GDCA 保留在这方面的法律权力。

If the assessment from a third-party auditor firm is completed, the audit results will be published at GDCA website (www.gdca.com.cn). Third-party should communicate its purposes and methods to GDCA in advance before notifying the evaluation entity on the assessment results or similar information, except otherwise defined by law, GDCA reserves the legal rights in this part.

8.7. 自评估 Self-Audits

见章节 8.1。

See section 8.1.

9. 法律责任和其他业务条款 Other Business and Legal Matters

9.1. 费用 Fees

GDCA 可根据提供的电子认证相关服务向本机构的证书订户收取费用，具体费用将取决于市场规则和相关管理部门的规定。

GDCA can charge subscriber certification fees for the digital authentication service provided. The specific charge will be determined by market rules and regulations of relevant administration department.

9.1.1. 证书新增和更新费用 Certificate Issuance or Renewal Fees

GDCA 对证书新增和更新的费用，公布在 GDCA 的网站 www.gdca.com.cn 上，供用户查询。

The fees of GDCA adding and renewing certificates are published in the website www.gdca.com for user to query.

如果 GDCA 签署的协议中指明的价格和 GDCA 公布的价格不一致，以协议中的价格为准。

If the price specified in GDCA agreement is different from the one published, the agreement price prevails.

9.1.2. 证书查询费用 Certificate Access Fees

对于证书查询，目前 GDCA 不收取任何费用。除非用户提出的特殊需求，需要 GDCA 支付额外的费用，GDCA 将与用户协商收取应该收取的费用。

Currently, GDCA doesn't charge for inquiry during the certificate validation period. Unless the subscriber has special requests, which makes GDCA to pay extra fees, GDCA will interact with the subscriber for appropriate charges.

如果证书查询的收费政策有任何变化，GDCA 将会及时在网站 www.gdca.com.cn 上予以公布。

If certificate inquiry charging policy has any changes, GDCA will promptly post the changes at its website (www.gdca.com.cn).

9.1.3. 撤销和状态信息查询费用 Revocation or Status Information Access Fees

对于撤销和状态信息查询，目前 GDCA 不收取任何费用。除非用户提出的特殊需求，需要 GDCA 支付额外的费用，GDCA 将与用户协商收取应该收取的费用。

GDCA currently does not charge any fees for the certificate revocation and status inquiry. Unless the subscriber has special requests, which makes GDCA to pay extra fees, GDCA will interact with the subscriber for appropriate charges.

如果撤销和状态信息查询的收费政策有任何变化，GDCA 将会及时在网站 www.gdca.com.cn 上予以公布。

If revocation and status information inquiry charging policy has any changes, GDCA will promptly post the changes at its website (www.gdca.com.cn).

9.1.4. 其他服务费用 Fees for Other Services

1. 如果用户向 GDCA 索取纸质的 CP 或其他相关的作业文件时，GDCA 需要收取因此产生的邮递和处理工本费。
2. GDCA 将向用户提供证书存储介质及相关服务，GDCA 在与订户或者其他实体签署

的协议中指明该项价格。

3. 其他 GDCA 将要或者可能提供的服务的费用，GDCA 将会及时公布，供用户查询。

1. If subscriber requests paper version of CP or other related documents from GDCA, GDCA will charge postage and processing fees.
2. GDCA provides certificate storage media and related services to subscribers. GDCA declares the prices of above items in the agreements signed with subscribers or other entities.
3. Other services fees that GDCA may or will charge will be published timely for referencing.

9.1.5. 退款策略 Refund Policy

GDCA 对订户收取的费用，除了证书申请和更新费用因为特定理由可以退还外，GDCA 均不退还用户任何费用。

GDCA does not refund any fees to subscribers except fees charged for certificate application and renewal because of specific reasons.

在实施证书操作和签发证书的过程中，GDCA 遵守严格的操作程序和策略。如果 GDCA 违背了本 CP 所规定的责任或其它重大义务，订户可以要求 GDCA 撤销证书并退款。在 GDCA 撤销了订户的证书后，GDCA 将立即把订户为申请该证书所支付的费用全额退还给订户。

In the process of the certificate operation and the certificate issuance, GDCA complies with strict operating procedures and policies. If GDCA violates its defined responsibilities under this CP or other material obligations, subscribers can request GDCA to revoke certificates and refund. After GDCA revokes subscriber's certificates, GDCA will immediately refund the full amount that subscribers have paid for the certificate application.

此退款策略不限制订户得到其它的赔偿。

This refund policy does not limit users from obtaining other compensation.

完成退款后，订户如果继续使用该证书，GDCA 将追究其法律责任。

After refund completion, if a subscriber continues to use the certificate, GDCA shall investigate his/her legal liabilities.

9.2. 财务责任 Financial Responsibility

9.2.1. 保险范围 Insurance Coverage

保险范围主要针对 CP 第 9.9 节中所规定的赔偿。

Insurance Coverage mainly focuses on compensation specified in CP Section 9.9.

9.2.2. 其他财产 Other Assets

不适用。

Not applicable.

9.2.3. 对最终实体的保险或担保范围

Insurance or Warranty Coverage for End-Entities

证书订户一旦接受 GDCA 的证书，或者通过协议完成对证书服务的接受，那么就意味着该订户已经接受了本 CP 关于保险和担保的规定和约束。

The acceptance of the certificate or its services specified by the agreement by the subscriber means that subscriber has accepted the specification and constraint of insurance and warranty coverage in this CP.

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 GDCA 提供的电子认证服务中，以下信息视为保密信息：

1. GDCA 订户的数字签名及解密密钥；
2. 审计记录包括：本地日志、服务器日志、归档日志的信息，这些信息被 GDCA 视为保密信息，只有安全审计员和业务管理员可以查看。除法律要求，不可在公司外部发布；
3. 其他由 GDCA 和 RA 保存的个人和公司信息应视为保密，除法律要求，不可公布。

In the electronic certification service provided by GDCA, the following information is treated as confidential information:

1. GDCA subscriber’s digital signature and decryption key
2. Audit records including local logs, server logs, archive logs information, which is treated by GDCA as confidential information. These records can only be accessed by security auditors and business administrators. Unless for law requirements, this information cannot be released outside of the company
3. Other individual and company information preserved by GDCA and RA and should be treated as confidential. Unless for law requirements, this information cannot be released to the public

9.3.2. 不属于保密的信息

Information Not Within the Scope of Confidential Information

1. 由 GDCA 发行的证书、证书中的公钥；

1. Certificate issued by GDCA and its public key.

2. 证书中的订户信息；

2. Information of subscriber in the certificate.

3. 证书撤销列表；

3. CRL

4. 证书策略（CP）、电子认证业务规则（CPS）。

4. CP and CPS

9.3.3. 保护保密信息的责任 Responsibility to Protect Confidential Information

GDCA、注册机构、订户以及与认证业务相关的参与方等，都有义务按照本 CP 的规定，承担相应的保护保密信息的责任，必须通过有效的技术手段和管理程序对其进行保护。

GDCA, RA, subscribers, relevant entities and parties involved in certification business, have the obligations to assume appropriate responsibility of keeping confidential information in accordance with this CP, and must protect it through effective technical means and management process.

当保密信息的所有者出于某种原因，要求 GDCA 公开或披露他所拥有的保密信息时，GDCA 应满足其要求；同时，GDCA 将要求该保密信息的所有者对这种申请进行书面授权，以表示其自身的公开或者披露的意愿。如果这种披露保密信息的行为涉及任何其他方的赔偿义务，GDCA 不应承担任何与此相关的或由于公开保密信息所造成的损失。保密信息的所有者应承担与此相关的或由于公开保密信息引起的所有赔偿责任。

As confidential-information holder requires GDCA to publish or reveal all his/her/its own confidential information due to some causes, GDCA shall satisfy his/her/its requirements; Also, GDCA shall require the holder’s documentary application and authorization to express his/her/its own will of publishing or revealing.
If any other obligation of compensation is involved in the act of revealing confidential information of the user by GDCA, GDCA will not assume any responsibility for damage concerning it or caused by the act of publishing the user's confidential information. The confidential-information holder shall assume compensatory responsibilities related with it or caused by the opening of confidential information.

当 GDCA 在任何法律、法规、法院以及其他公权力部门通过合法程序的要求下，必须提供本 CP 中规定的保密信息时，GDCA 应按照法律、法规以及法院判决的要求，向执法部门

公布相关的保密信息，GDCA 无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

When facing any requirements of laws and regulations or any demands for undergoing legal process of court and other agencies, GDCA must provide confidential information in this CP, and could publish the relevant confidential information to law-enforcing department according to requirements of laws, regulations, legal doctrines or court judgments. Under this circumstance, GDCA shall not assume any responsibility. The reveal shall not be regarded as a breach of confidential requirement and obligations.

9.4. 个人隐私保密 Privacy of Personal Information

9.4.1. 隐私保密计划 Privacy Plan

GDCA 应制定隐私保密计划对订户的个人信息保密。

GDCA should establish the Non-disclosure plan to protect the privacy information of subscriber.

9.4.2. 作为隐私处理的信息 Information Treated as Private

除了证书中已经包括的信息以及证书状态信息外，订户提供的其他基本信息将被视为隐私处理。作为隐私处理的信息包括：

Except for the information already included in the subscriber certificates and the certificate status information, other basic information provided by the subscribers is deemed private. Information treated as private includes:

1. 订户的有效证件号码如身份证号码、单位机构代码；
2. 订户的联系电话；
3. 订户的地址；
4. 订户的银行帐号。

1. Subscriber’s valid documents number such as ID number, organization code
2. Subscriber's telephone number
3. Subscriber’s mailing address and living address
4. Subscriber's bank account number

9.4.3. 不被认为隐私的信息 Information Not Deemed Private

订户持有的证书内包括的信息，以及该证书的状态等，是可以公开的，不被视为隐私信息。

All information in a subscriber certificate and the status information of the certificate, etc. is deemed not private, and shall not be regarded as privacy information.

9.4.4. 保护隐私的责任 Responsibility to Protect Private Information

GDCA、注册机构有妥善保管与保护本 CP 第 9.4.2 节中规定的订户隐私信息的责任与义务。

GDCA has the responsibility and obligation for proper custody and protection of the certificate applicant personal privacy described in section 9.4.2.

9.4.5. 使用隐私信息的告知与同意 Notice and Consent to Use Private Information

GDCA 在其认证业务范围内使用所获得的任何订户信息，只用于订户身份识别、管理和服务订户的目的。在使用这些信息时，无论是否涉及到隐私，GDCA 都没有告知订户的义务，也无需得到订户的同意。

Any subscriber information GDCA obtaining within the scope of certification business can only be used for identifying, managing and serving subscribers. When using the information, no matter the privacy is involved or not, GDCA has no obligations to notify subscribers, and no need to obtain subscriber's consent.

GDCA 在任何法律法规或者法院以及公权力部门通过合法程序的要求下，或者信息所有者书面授权的情况下向特定对象披露隐私信息时，也没有告知订户的义务，并且不需得到订户的同意。

Under any requirements of laws and regulations, and demands for undergoing the legal process of other agencies, or under the circumstance where private information holder submits the written authorization to certain object for publishing the information, GDCA has no obligations to notify subscriber, and to obtain the consent from the subscriber.

GDCA、注册机构如果需要将订户隐私信息用于双方约定的用途以外的目的，事前必须告知订户并获得订户同意和授权，而且这种同意和授权要用可归档的方式（如传真、信函等）。

If GDCA and registration authority shall apply user's private information to other purposes beyond the functions agreed between two sides, CA and RA shall notify subscriber to obtain his/her/its agreement and authorization, and the agreement and authorization shall be in the form which can be archived (such as fax and business letters etc.).

9.4.6. 依法律或行政程序的信息披露

Disclosure Pursuant to Judicial or Administrative Process

由于法律执行、法律授权的行政执行的需要，GDCA 将订户的隐私信息提供给有关执法机关、行政执行机关是允许的。包括：

Due to the need of legal execution as well as administrative execution permitted by legal authorization, GDCA shall provide subscriber's private information to relevant law enforcement agency and administrative enforcement authorities. The above behaviors are permitted. It includes:

1. 政府法律法规的规定并且经相关部门通过合法程序提出申请；

1. Submit the application following the legal process required by relevant agencies pursuant to the provisions of laws and regulations.

2. 法院以及公权力部门处理因使用证书产生的纠纷时合法的提出申请；

2. The formal application by court and other agencies when dealing with the dispute of using certificate

3. 具有合法司法管辖权的仲裁机构的正式申请。

3. The formal application by arbitration agency with legal jurisdiction。

9.4.7. 其他信息披露情形 Other Information Disclosure Circumstances

如果订户要求 GDCA 提供某类特定客户支援服务如资料邮寄时，GDCA 则需要把订户的联系电话和地址等信息提供给第三者如邮寄公司。

If certificate subscriber requires GDCA to provide some particular customer support services such as mailing materials, GDCA needs to send the subscriber's name, mailing address and other related information to a third-party such as mailing company.

9.5. 知识产权 Intellectual Property Rights

1. GDCA 享有并保留对证书以及 GDCA 提供的所有软件的全部知识产权；
2. GDCA 对数字证书系统软件具有所有权、名称权、利益分享权；
3. GDCA 网站上公布的一切信息均为 GDCA 财产，未经 GDCA 书面允许，他人不能转载用于商业行为；
4. GDCA 发行的证书和 CRL 均为受 GDCA 支配的财产；
5. 对外运营管理策略和规范为 GDCA 财产；
6. 用来表示目录中 GDCA 域中的实体的甄别名（以下简称 DN）以及该域中颁发给终端实体的证书，均为 GDCA 的财产。

1. GDCA reserves and remains full intellectual properties rights for all the certificates and software offered by GDCA.
2. GDCA holds ownership, the right of name, the right to share the benefits for certificate system software
3. All the information published at GDCA website is GDCA property. Without written permission of GDCA, others cannot repost them for commercial activities.
4. Certificates and CRLs issued by GDCA are both the properties controlled by GDCA.
5. External operation management strategy and specification are GDCA property.
6. The distinguished name (hereinafter referred to as DN) used to express the GDCA domain entity in the directory and the certificate issued to the terminal in the domain entity are the properties of GDCA.

9.6. 陈述与担保 Representations and Warranties

9.6.1. CA 的陈述与担保 CA Representations and Warranties

GDCA 对证书订户必须做出如下担保：

GDCA must make the following warranties to subscriber:

1. GDCA 签发给订户的证书符合本 CP 的所有实质性要求；

1. Certificates issued to subscribers by GDCA must be in line with all substantive requirements of this CP.

2. 验证证书中所包含的全部信息的准确性（organizationalUnitName 信息除外）；

2. Verifies the accuracy of all of the information contained in the certificate (with the exception of the organizationalUnitName information).

3. GDCA 保证其私钥得到安全的存放和保护，GDCA 建立和执行的安全机制符合国家相关政策的规定；

3. GDCA ensures that its private key shall be stored and protected securely, and GDCA shall establish and implement security mechanism pursuant to the terms of national relevant policies.

4. GDCA 将按本 CP 的规定，及时撤销证书；

4. GDCA shall revoke certificate timely in accordance with this CP.

5. GDCA 将向证书订户通报任何已知的，将在本质上影响订户的证书的有效性和可靠性事件。

5. GDCA informs subscribers any known events, which will fundamentally affect the validity and reliability of the certificate.

6. 验证申请者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

有域名使用权或控制权人士的授权）中的域名及 IP 地址拥有使用权或控制权；

6. Verifies that the applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control);

7. 验证申请者授权了证书的签发以及申请者代表获得了授权，以代表申请者申请证书；

7. Verifies that the applicant authorized the issuance of the certificate and that the applicant representative is authorized to request the certificate on behalf of the applicant;

8. 采取验证措施以减小证书主题“organizationalUnitName”中所包含的信息存在误导的可能性；

8. Implements a procedure for reducing the likelihood that the information contained in the certificate's subject: organizationalUnitName attribute would be misleading;

9. 根据 CP 3.2 的要求验证申请人的身份；

9. Verifies the identity of the applicant according to section 3.2 of this CP;

10. 若 GDCA 与订户无关联，则 GDCA 与订户是合法有效且可执行的订户协议双方，该订户协议符合 CA/浏览器论坛发布的 Baseline Requirements 等要求；若 GDCA 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；

10. That, if GDCA and subscribers are not affiliated, the subscriber and GDCA are parties to a legally valid and enforceable subscriber agreement that satisfies the Baseline Requirements and other requirements published by the CA/Browser Forum, or, if GDCA and subscribers are the same entity or are affiliated, the applicant representative acknowledged the terms of use;

11. 针对所有未过期的证书的当前状态信息（有效或已撤销）建立及维护全天候的（24x7）公开的信息库。

11. Maintains a 24 x 7 publicly-accessible repository with current information regarding the status (valid or revoked) of all unexpired certificates.

GDCA 对依赖方必须做出如下担保：

GDCA must make the following warranties to relying party:

1. 证书中的信息都是经过验证的；

1. GDCA guarantees that the information contained in the certificate has been properly validated.

2. GDCA 完全遵照本 CP 及 CPS 的规定签发证书；

2. GDCA is in full compliance with the provisions of the CP and relevant CPS to issue certificate.

3. 在 GDCA 信息库中发布的证书已经签发给了订户，并且订户已经按照本 CP 中的规定接受了该证书。

3. Certificates published in GDCA repositories should have been issued to subscribers and accepted

by subscribers in accordance with the provisions of the CP.

9.6.2. RA 的陈述与担保 RA Representations and Warranties

1. 提供给证书订户的注册过程完全符合本 CP 的所有实质性要求；
2. 在 GDCA 生成证书时，不会因为注册机构的失误而导致证书中的信息与证书申请者的信息不一致；
3. 注册机构将按本 CP 的规定，及时向 GDCA 提交证书申请、撤销、更新等服务申请。

1. The registration process provided for subscribers is compliant with all the substantive requirements of GDCA CP.
2. When generating certificates, GDCA does not allow the inconsistencies between certificate information and certificate applicant information due to mistakes of registration authority.
3. Registration authority will submit the applications of revocation, update and other services to GDCA in time according to the provisions of CP.

9.6.3. 订户的陈述与担保 Subscriber Representations and Warranties

订户一旦接受GDCA签发的证书，就被视为向GDCA、注册机构及依赖方作出以下承诺：

1. 在证书的有效期内进行数字签名；
2. 订户在申请证书时向注册机构提供的信息都是真实、完整和准确的，愿意承担任何提供虚假、伪造等信息的法律责任；
3. 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 GDCA 或其授权的证书服务机构；
4. 与订户证书所含公钥相对应的私钥所进行的每一次签名，都是订户自己的签名，并且在进行签名时，证书是有效证书（证书没有过期、撤销），证书的私钥为订户本身访问和使用；
5. 除非经订户和发证机构间书面协议明确规定，订户保证不从事发证机构（或类似机构）所从事的业务；
6. 一经接受证书，即表示订户知悉和接受本 CP 中的所有条款和条件，并知悉和接受相应的订户协议；
7. 一经接受证书，订户就应当承当如下责任：始终保持对其私钥的控制，使用可信的系统，采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用；
8. 不得拒绝任何来自 GDCA 公示过的声明、改变、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；

9. 证书在本 CP 中规定使用范围内合法使用，只将证书用于经过授权的或其他合法的使用目的；
10. 采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件；
11. 对于 SSL/TLS 证书，订户有责任和义务保证只在证书中列出的主题别名对应的服务器中部署证书；
12. 对于代码签名证书，订户不得将其用于可疑代码等非法软件、恶意软件的签名。

Once subscribers accept a certificate issued by GDCA, the subscriber is considered to make the following commitments to GDCA, registration authority and related parties who trust the certificate:

1. The subscriber uses digital signatures if the certificate is valid.
2. All information that subscriber provides to registration authority during certificate application process must be true, complete and accurate. The subscriber is willing to take legal responsibility for any false or forged information.
3. If there is an agent, then both the subscriber and agent take jointly responsibility. The subscriber is responsible for notifying GDCA and its authorized certification services agencies any false statements and omissions made by the agent.
4. Each signature is generated using the private key corresponding to certificate by subscribers themselves. The certificates shall be valid at the moment of signing, i.e. certificate is not revoked or expired.
5. Subscribers ensure that they don't engage in business performed by the issuing agency (or similar institutions) unless they sign written agreements with the issuing agency on such matters.
6. Once the certificate is accepted, subscribers are considered as knowing and accepting all the terms and conditions in the CP as well as corresponding subscriber agreements.
7. Once the certificate is accepted, the subscriber should assume the following responsibilities: always maintain control of their private keys; use trust worthy systems; and take reasonable precautions to prevent the loss, disclosure, alteration, or unauthorized usage of the private keys.
8. Prohibited for rejecting any statements, changes, updates and upgrades published by GDCA, including but not limited to modification of strategies and standards as well as additions and deletions of certificate services.
9. The subscriber only uses certificate for the authorized or other lawful purpose within the range specified by this CP.
10. The subscriber use secure and reasonable measures to prevent the private key from loss, disclosure, alteration and other events.
11. For the SSL/TLS certificates, the subscribers undertake an obligation and warranty to install the certificates only on servers that are accessible at the subjectAltName(s) listed in the certificates.
12. The subscriber must not use the code signing certificates for signing suspicious codes and other illegal or malicious software.

9.6.4. 依赖方的陈述与担保 Relying Party Representations and Warranties

1. 遵守本 CP 的所有规定；
2. 在依赖证书前，确认证书在规定的范围和期限使用；
3. 在依赖证书前，对证书的信任链进行验证；
4. 在依赖证书前，通过查询 CRL 或 OCSP 确认证书是否被撤销；
5. 一旦由于疏忽或者其他原因违背了合理检查的条款，依赖方愿意就此而给 GDCA 带来的损失进行补偿，并且承担因此造成的自身或他人的损失；
6. 不得拒绝任何来自 GDCA 公示过的声明、改变、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。

1. Abide by all provisions of this CP.
2. Ensure that the certificate is used in prescribed scope and duration.
3. Verify certificate's trust chain before trust the certificate.
4. Before trust a certificate, verify whether the certificate is revoked or not through querying CRL or OCSP.
5. The relying party is willing to compensate GDCA for the losses and accept liabilities for any loss of self or others, due to negligence or other reasons violating the terms of a reasonable inspection.
6. Prohibited for rejecting any statements, changes, updates and upgrades published by GDCA, including but not limited to modification of strategies and standards as well as additions and deletions of certificate services.

9.6.5. 其他参与者的陈述与担保

Representations and Warranties of Other Participants

遵守本 CP 的所有规定。

Abide by all provisions of this CP.

9.7. 担保免责 Disclaimers of Warranties

除本 CP 9.6.1 中的明确承诺外，GDCA 不承担其他任何形式的保证和义务：

1. 不保证证书订户、依赖方、其他参与者的陈述内容；
2. 不对电子认证活动中使用的任何软件做出保证；
3. 不对证书在超出规定目的以外的应用承担任何责任；

4. 对由于不可抗力，如战争、自然灾害等造成的服务中断并由此造成的客户损失承担责任；
5. 订户违反本 CP9.6.3 之承诺时，或依赖方违反本 CP9.6.4 之承诺时，得以免除 GDCA 之责任。

Except for the commitments declared in CP Section 9.6.1, GDCA does not assume any other forms of guarantee and obligation:

1. Do not guarantee the statements of certificate subscribers, relying party and other.
2. Do not guarantee any software used in electronic certification activities.
3. Do not assume any liability when certificate is used beyond the prescribed purposes.
4. Do not assume any responsibility for service interruption and customer losses caused by force majeure, such as war, natural disasters, etc.
5. When subscriber violates the commitments defined in CP Section 9.6.3, or relying party violates the commitments defined in CP Section 9.6.4, GDCA can exempt from liability.

9.8. 有限责任 Limitations of Liability

证书订户、依赖方因 GDCA 提供的电子认证服务从事民事活动遭受损失，GDCA 只承担本 CP 第 9.9.1 节规定的有限责任。

The certificate subscriber and the relying party specialized in civil activities suffered losses due to electronic certification service provided by GDCA, GDCA only assume limited liability amount stipulated in CP section 9.9.1.

9.9. 赔偿 Indemnities

9.9.1. 认证机构的赔偿责任 Indemnification by GDCA

如 GDCA 违反了本 CP 第 9.6.1 节中的陈述，订户、依赖方等实体可申请 GDCA 承担赔偿责任（法定或约定免责除外），包括以下情形：

1. GDCA 将证书错误的签发给订户以外的第三方，导致订户或依赖方遭受损失的；
2. 在订户提交信息或资料准确、属实的情况下，GDCA 签发的证书出现了错误信息，导致订户或依赖方遭受损失的；
3. 在 GDCA 明知订户提交信息或资料存在虚假谎报的情况，但仍然向订户签发证书，导致依赖方遭受损失的；
4. 由于 GDCA 的原因导致 CA 私钥的泄露；

5. GDCA 未能及时撤销证书，导致依赖方遭受损失的。

If GDCA violates statements in CP Section 9.6.1, certificate subscribers, relying parties and other entities can request GDCA assume compensation liabilities (except for statutory and contractual exemptions). If the following circumstances occur, GDCA will assume limited compensation liability:

1. GDCA issues certificates to a third-party instead of the subscriber by mistake, which leads to losses of the subscriber or relying party.
2. If subscriber submits accurate and true information to GDCA, but GDCA issues certificates with error information and the error leads to losses of the subscriber or relying party.
3. After GDCA knows the fact that subscriber provides fake registration information or data, GDCA still issues certificate, which leads to relying party suffering losses.
4. If the private key of CA is disclosed due to GDCA's fault.
5. GDCA fails to revoke certificates in time, which leads to relying party suffering losses.

9.9.2. 订户的赔偿责任 Indemnification by Subscribers

在如下情况，订户对自身原因造成的 GDCA、依赖方损失，应当承担赔偿责任：

If the following situations cause GDCA or relying party suffering losses, subscribers shall be assumed the liability to compensate:

1. 订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致 GDCA 及其授权的证书服务机构或者第三方遭受损害；
2. 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知 GDCA 及其授权的证书服务机构，以及不当交付他人使用造成 GDCA 及其授权的证书服务机构、第三方遭受损害；
3. 订户使用证书的行为，有违反本 CP 及相关操作规范，或者将证书用于非本 CP 规定的业务范围；
4. 证书订户或者其它有权提出撤销证书的实体提出撤销请求后，到 GDCA 将该证书撤销信息予以发布的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果 GDCA 按照本 CP 的规范进行了有关操作，那么该证书订户必须承担所有损害赔偿责任；
5. 证书中的信息发生变更但未停止使用证书并及时通知 GDCA 和依赖方；
6. 没有对私钥采取有效的保护措施，导致私钥丢失或被损害、窃取、泄露等；
7. 在得知私钥丢失或存在危险时，未停止使用证书并及时通知 GDCA 和依赖方；
8. 证书到期但仍在使用证书；

9. 订户的证书信息侵犯了第三方的知识产权；
10. 在规定的应用范围外使用证书，如从事违法犯罪活动。

1. GDCA and its authorized service agencies or third-party suffer losses due to unreal information, such as deliberate, negligent or malicious provision of unreal information by applicants when applying for certificates.
2. GDCA and its authorized service agencies or third-party suffer losses due to disclosure and loss of private keys deliberately and by mistake; due to not informing GDCA and its authorized service agencies or third-party of the leakage and loss of private keys with knowing the facts; and due to handing keys to others inappropriately.
3. Subscribers violate the CP and related operation practices when using certificates as well as using the certificates activities outside of the CP.
4. If the certificate is used for illegal transactions or causes disputes during the period from revocation requests submitted by the subscribers or other entities authorized by GDCA to this information of certificate revocation published by GDCA, if GDCA operates in accordance with the requirements of the CP, subscribers must assume any responsibility of losses according to this CP.
5. Subscribers do not stop to use the certificate which its information have changed and don't notify it to GDCA or relying parties in time.
6. The private key is lost, compromised, stolen, exposed, and etc. due to not taking effective protection measures.
7. Subscribers continue to use the certificates and do not notify GDCA and relying parties promptly when they are made aware that private keys are lost or at the risk of being compromised.
8. The certificate has expired but is still in use.
9. The subscriber’s certificate information infringes upon the intellectual property rights of a third-party.
10. Using certificates outside the provisions of specific application scope, such as the use of certificates for illegal and criminal activities.

9.9.3. 依赖方的赔偿责任 Indemnification by Relying Parties

在如下情况，依赖方对自身原因造成的 GDCA、订户损失，应当承担赔偿责任：

If the following circumstances lead to the losses of GDCA or subscriber, relying party shall be assumed responsibility to compensate:

1. 没有履行 GDCA 与依赖方的协议和本 CP 中规定的义务；
2. 未能依照本 CP 规范进行合理审核，导致 GDCA 及其授权的证书服务机构或第三方遭受损害；
3. 在不合理的情形下依赖证书，如依赖方明知证书存在超范围、超期限使用的情形或证书已经或有可能被人窃取的情形，但仍然依赖证书；

4. 依赖方没有对证书的信任链进行验证；
5. 依赖方没有通过查询 CRL 或 OCSP 确认证书是否被撤销。

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

9.10. 有效期与终止 Term and Termination

9.10.1. 有效期 Term

本 CP 在发布日期零时正式生效，上一版本的 CP 同时失效；本 CP 在下一版本 CP 生效之日或在 GDCA 终止电子认证服务时失效。

This CP will enter into force at 12 o'clock of the release date, and the last version CP will become invalid. This CP will become invalid when the next version CP enters into force or the electronic certification services of GDCA are terminated.

9.10.2. 终止 Termination

GDCA 终止电子认证服务时，本 CP 终止。

When GDCA terminates electronic certification services, this CP is terminated.

9.10.3. 终止的效果与存续 Effect of Termination and Survival

本 CP 的终止，意味着认证机构认证业务的终止，但认证业务的终止不意味着认证机构责任的终止。认证机构在业务终止后应采取合理的措施，将认证服务转到其他认证机构，保证订户的利益。

The termination of this CP means that the termination of CA business, but the termination of certification business does not mean the termination of CA's responsibility. After the termination of business, CA shall take reasonable measures to transfer certification service to other CA so as to ensure the interests of the subscriber.

9.11. 对参与者的个别通告及信息交互

Individual Notices and Communications with Participants

认证机构在必要的情况下，如主动撤销订户证书、发现订户将证书用于规定外用途及订户其他违反订户协议的行为，可通过适当方式，如电话、电子邮件、信函等，个别通知订户、依赖方。

The circumstances that CA actively revokes the subscriber's certificate, finds out subscriber using certificate out of specified usage, or behaviors of subscriber violating subscriber agreement have occurred, CA can use appropriate way, such as telephone, E-mail, letter, Fax, etc., to notify subscriber and relying party if necessary.

9.12. 修订 Amendments

9.12.1. 修订程序 Procedure for Amendment

经 GDCA 安全策略委员会授权，CPS 编写小组每年至少审查一次本 CP，确保其符合国家法律法规、主管部门的要求以及相关国际标准，符合认证业务开展的实际需要。

Through the authorization of GDCA Security Policy Committee, CPS composition team shall review this CP at least once a year, to ensure that CP meets the requirements of national laws and regulations and administration department, to meet the latest SSL baseline requirements and specifications, and satisfy the actual requirements of certification business operation.

本 CP 的修订，由 CPS 编写小组提出修订报告，获得 GDCA 安全策略委员会批准后，由 CPS 编写小组负责组织修订，修订后的 CP 经过 GDCA 安全策略委员会批准后正式对外发布。

The revised version of this CP will be revised by the CPS composition team and approved by GDCA Security Policy Committee. CPS composition team will be responsible for the revision and the revised CP will be officially released after being approved by the GDCA Security Policy Committee.

9.12.2. 通知机制和期限 Notification Mechanism and Period

修订后的 CP 经批准后将立即在 GDCA 的网站 https://www.gdca.com.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，GDCA 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。

After approval of the revised CP, it will be posted on GDCA official website https://www.gdca.com.cn immediately. For the modification notified by email, mail, media and other ways, GDCA shall notify the relevant parties in reasonable time, which ensures that the relevant parties have minimum influence.

9.12.3. 必须 OID 的情形 Circumstances Under Which OID Must be Changed

GDCA 负责确定 CP 的修订是否需要修改 OID。

GDCA is responsible for determining whether an amendment to the CP requires an OID change.

9.13. 争议解决条款 Dispute Resolution Provisions

当 GDCA、订户和依赖方之间出现争议时，有关方面应依据协议通过协商解决，协商解决不了的，可通过法律解决。

Any disputes between GDCA and subscribers or relying parties shall be resolved through negotiations as agreed, and those cannot be settled by negotiations will be resolved by laws.

9.14. 管辖法律 Governing Law

GDCA 的 CP 受国家已颁布的《中国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》法律法规管辖。

The CP of GDCA is governed by the law of “Electronic Signatures Laws of People’s Republic of China”, the regulation of “Measures for the Administration of Electronic Certification Services” and “Measures for the Administration of Cipher Codes for Electronic Certification Services” promulgated by the country.

9.15. 符合适用法律 Compliance with Applicable Law

认证机构的所有业务、活动、合同、协议必须符合《中国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》以及其它中华人民共和国法律法规的规定。

All businesses, activities, contracts, and agreements of GDCA must conform to "Electronic Signatures Laws of People’s Republic of China”, “Measures for the Administration of Electronic Certification Services”, “Measures for the Administration of Cipher Codes for Electronic Certification Services” and other laws and regulations of People’s Republic of China.

9.16. 一般条款 Miscellaneous Provisions

9.16.1. 完整协议 Entire Agreement

CP、CPS、订户协议、依赖方协议及其补充协议将构成 PKI 参入者之间的完整协议。

The entire agreement is composed of CP, CPS, Subscriber Agreement and Relying Party Agreement as well as its supplementary agreement.

9.16.2. 让渡 Assignment

根据本 CP 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的相关规定进行权利和义务的转让。此转让行为发生时不影响到转让方对另一方的任何债务及责任的更新。

According to the rights and obligations of certification entity parties detailed in this CP, all parties can transfer the possession of rights and obligations in accordance with the relevant provisions of the law. The occurrence of the above transfer behavior does not affect the change of any debt and liability among the transferors.

9.16.3. 分割性 Severability

如果本 CP 的任何条款或其应用由于与 GDCA 所在管辖区的法律产生冲突而被判定为无效或不具执行力时 ，GDCA 应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，GDCA 应在此章节批露修订的内容。

在根据修订后要求签发证书之前，GDCA 应发送邮件至 question@cabforum.org， 通知 CAB 论坛 CP 中已修订的信息，并确认其已被发至公共邮件列表和存在于公共档案列表 (https://cabforum.org/pipermail/public/)。

若法律不再适用，或 CA/B 论坛的要求被修改，使 GDCA 同时符合 CA/B 论坛的 Baseline Requirements 及法律要求，则本章节中任何对 GDCA 业务操作的调整应不再继续适用。上述对业务操作进行的相关调整，对 GDCA 的 CP 的修订，及向 CA/B 论坛的通知应在 90 天内完成。

In case any clause or provision of this CP is held to be unenforceable or invalid due to any conflicts with the laws of any jurisdiction in which GDCA operates, GDCA shall modify any conflicting clause or provision to the minimum extent necessary to make them continue to be valid, and other clauses and provisions shall remain valid without being affected. GDCA shall disclose the modified contents in this section.

GDCA shall (and prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of any modified content in the CP by sending emails to question@cabforum.org, and confirm that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/.

Any modification to GDCA's practice enabled under this section shall be discontinued if and when the law no longer applies, or the requirements published by the CA/B Forum are modified to make it possible to comply with both them and the law simultaneously. An appropriate change in practice, modification to the GDCA's CP and a notice to the CA/Browser Forum, as outlined above, shall be made within 90 days.

9.16.4. 强制执行（律师费用和权利放弃）Enforcement (Attorneys' Fees and Waiver of Rights)

不适用。

Not applicable.

9.16.5. 不可抗力 Force Majeure

依据本 CP 制定的 CPS 应包括不可抗力条款，以保护各方利益。

CPS formulated in accordance with this CP shall include a force majeure clause to defend the benefits of each party.

9.17. 其他条款 Other Provisions

GDCA 对本 CP 具有最终解释权。

GDCA has final interpretation rights to this CP.

附录：GDCA 证书策略修订记录表

Appendix: GDCA CP Revision Records

内容 / 序号	修订章节	V3.3	V3.4
1	1.1.4. GDCA 证书层次架构 Hierarchical Architecture of GDCA Certificates		新增新签的代码签名中级 CA。
2	1.4.2. 限制的证书应用 Prohibited Certificate Uses		添加测试证书签发的相关说明。
3	3.2.9. 域名的确认和鉴别 Domain name recognition and identification		针对需要使用多视角签发验证的域名验证方法进行说明。增加关于 DNSSEC 验证相关要求。
4	3.2.12. IP 地址的确认和鉴别 Authentication of an IP Address		针对需要使用多视角签发验证的 IP 地址验证方法进行说明。
5	3.2.17. 多视角签发验证 Multi-Perspective Issuance Corroboration		增加多视角签发验证要求。
6	4.2.4. 认证机构授权（CAA） Certification Authority Authorization (CAA)		增加关于 DNSSEC 验证相关要求。
7	5.4.1. 记录事件的类型 Types of Events Recorded		增加防火墙和路由器活动日志记录要求。
8	6.7. 网络的安全控制 Network Security Controls		增加漏洞处理时限管理。
9	其他修订		调整个别措辞问题。

Content / SEQ	Sections Revised	V3.3	V3.4
1	1.1.4. GDCA 证书层次架构 Hierarchical		Add a new code signing Subordinate CA certificate.

	Architecture of GDCA Certificates		
2	1.4.2. 限制的证书应用 Prohibited Certificate Uses		Add descriptions related to the issuance of test certificates.
3	3.2.9. 域名的确认和鉴别 Domain name recognition and identification		Describe the domain validation methods that require the use of Multi-Perspective Issuance Corroboration. Add requirements related to DNSSEC validation.
4	3.2.12. IP 地址的确认和鉴别 Authentication of an IP Address		Describe the IP address validation methods that require the use of Multi-Perspective Issuance Corroboration.
5	3.2.17. 多视角签发验证 Multi-Perspective Issuance Corroboration		Add the requirements for Multi-Perspective Issuance Corroboration.
6	4.2.4. 认证机构授权（CAA） Certification Authority Authorization (CAA)		Add requirements related to DNSSEC validation.
7	5.4.1. 记录事件的类型 Types of Events Recorded		Add the requirements for the logging of router and firewall activities.
8	6.7. 网络的安全控制 Network Security Controls		Add management of vulnerability remediation timelines.
9	Other revisions		Adjust some wording issues.