数安时代科技股份有限公司

电子认证业务规则

版本：6.3

发布日期：2025 年 11 月 5 日

Global Digital Cybersecurity Authority CO., LTD.

Certification Practice Statement (CPS)

Version: 6.3

Release Date: November 5, 2025

目录

Contents

1. 概括性描述 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，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 granted the "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 and all the rights and obligations of the contracts and agreement 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 电子认证业务规则（CPS）Certification Practice Statement (CPS)

本电子认证业务规则（简称 CPS）根据《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》等法律法规的要求，详细阐述了 GDCA 提供的电子认证服务整个过程、电子认证服务所遵循的规则以及电子认证服务相关参与者所承担的责任。本 CPS 由 GDCA 通过公开发布的形式告知电子签名订户、依赖方和其他相关参与者，以确保 GDCA 所提供的电子认证服务是合法、专业、权威的第三方电子认证服务。对于 GDCA 所提供电子认证服务过程的责任范围，本 CPS 也给予了明确的规定。

Pursuant to the requirements of the “Electronic Signature Law of the 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 related laws and regulations, this Certification Practice Statement (abbreviated as CPS) outlines the overall processes that GDCA employs to provide electronic authentication services, illustrates the set of rules that GDCA conforms to in offering the electronic authentication service, and elaborates on the responsibilities undertaken by the participants of such services. GDCA makes this CPS available to the subscribers, relying parties and other relevant participants through open publication to ensure the validity, professionalism, and authority of GDCA’s electronic authentication services. This CPS also clearly defines the limitation of liabilities for the electronic authentication services provided by GDCA.

本 CPS 所阐述的内容遵循《GDCA 证书策略》(http://www.gdca.com.cn/cp/cp)，同时也遵循《粤港电子签名证书互认证书策略（1.1 版本）》（http://gdii.gd.gov.cn/xxh3236/content/post_945261.html）。在执行本 CPS 的过程中，

《GDCA 证书策略》与《粤港电子签名证书互认证书策略》存在不一致的内容应按以下规则处理：应用于粤港跨境互认的证书遵循《粤港电子签名证书互认证书策略》，应用于除粤港跨境互认外的证书遵循《GDCA 证书策略》。证书是否应用于粤港跨境互认项目可根据证书策略的对象标识符进行辨别。

This CPS conforms to both "GDCA Certificate Policy" (http://www.gdca.com.cn/cp/cp) and "Certificate Policy for Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong (version 1.1)" (http://gdii.gd.gov.cn/xxh3236/content/post_945261.html). The following principle shall prevail in case of any conflicts exist between the above two policies: the certificates applied to mutual recognition of electronic signature certificates issued by Hong Kong and Guangdong conform to " Certificate Policy for Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong", while other certificates conform to "GDCA Certificate Policy". Whether a certificate is applied to the project of “Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong” can be determined by the object identifier of certificate policy.

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 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任的 SSL/TLS 证书和、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 CPS，如果本 CPS 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。

GDCA conforms to the latest versions of the Baseline Requirements 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 CPS according to these updates. The specifications of the CA/Browser Forum shall prevail in case of any discrepancies between the provisions of this CPS and the standard specifications published by the CA/Browser Forum.

依据 IETF PKIX RFC 3647 CP/CPS 框架，本 CPS 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。

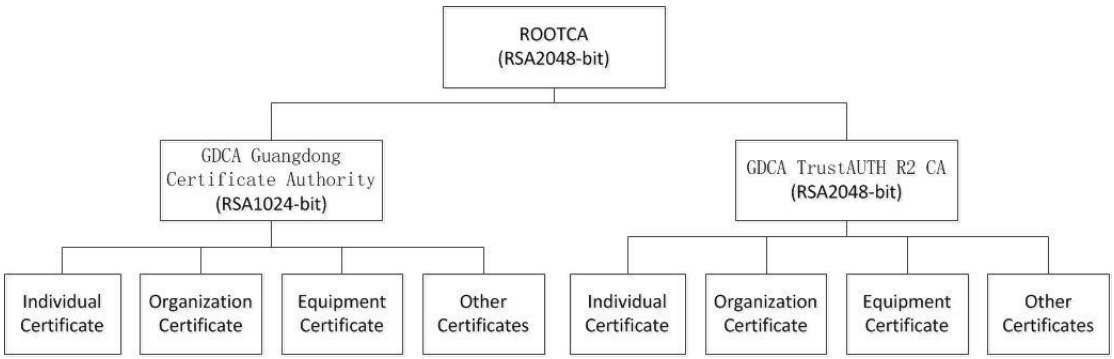
Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CPS is divided into nine parts that cover the security controls and practices and procedures for GDCA's certificate services. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement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

1.1.3 GDCA 证书层次架构 GDCA Certificate Hierarchical Architecture

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, 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.

ROOTCA (RSA)证书将于 2025 年 8 月 23 日到期。

ROOTCA (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.

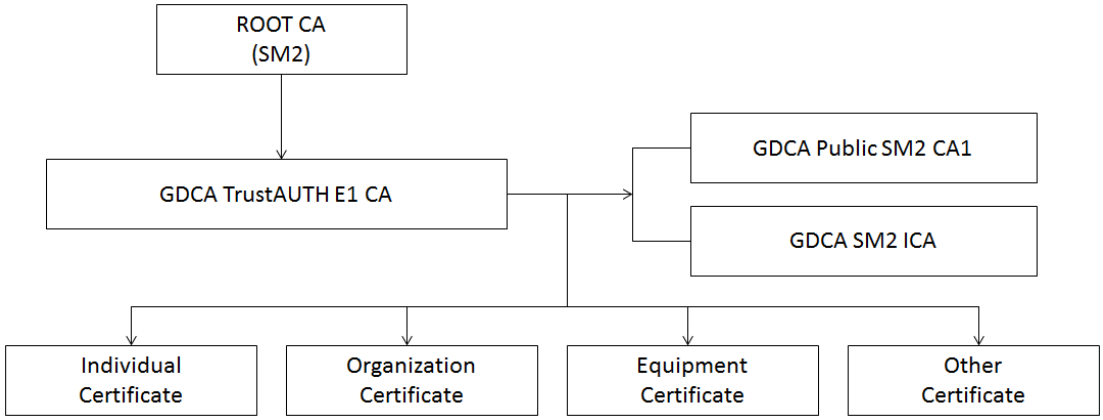
GDCA ROOT CA 证书于 2024 年 12 月 11 日到期。

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 used 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.

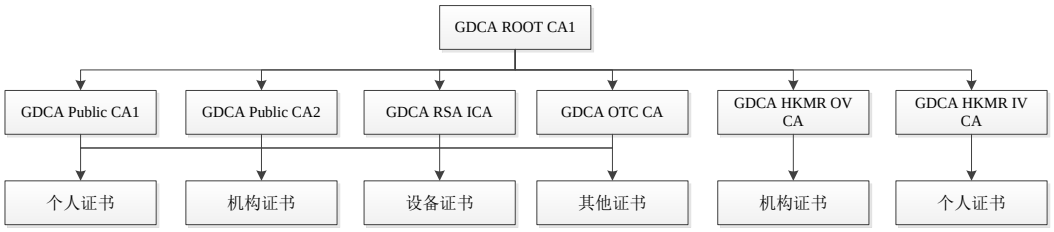
GDCA SM2 ICA 证书将在2033年12月31日到期，2030 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

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。

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.

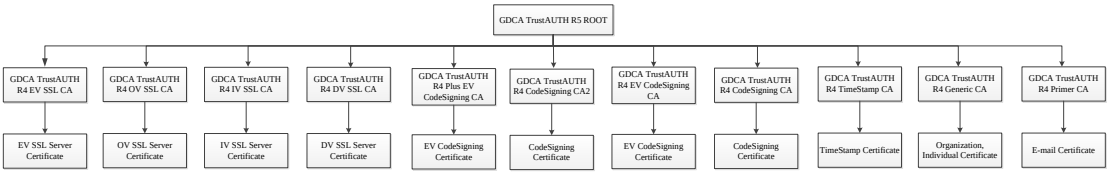
GDCA HKMR OV CA will expire on December 31, 2030, and from January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

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.

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 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 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 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 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 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 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 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 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 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 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 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 R5 ROOT certificate will expire on December 31, 2040.

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

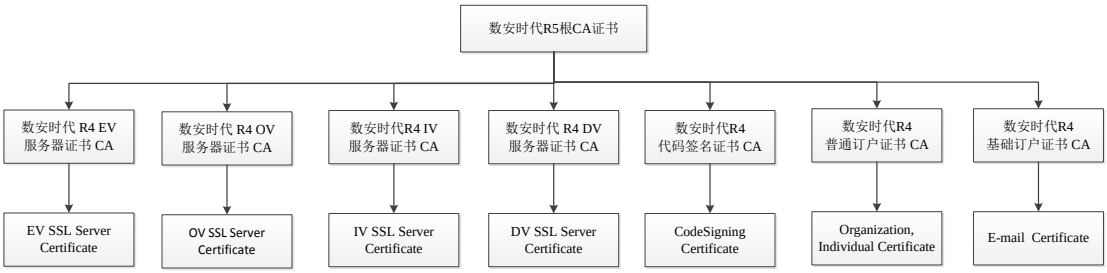
GDCA TrustAUTH R4 CodeSigning CA certificate will expire on December 31, 2030. As of June 1, 2021, GDCA has stopped the issucane of subscriber certificates with this CA certificate.

GDCA TrustAUTH R4 TimeStamp CA 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 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 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 RSA2048-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 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 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 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 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 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 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 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 R5 根 CA certificate will expire on December 31, 2040.

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

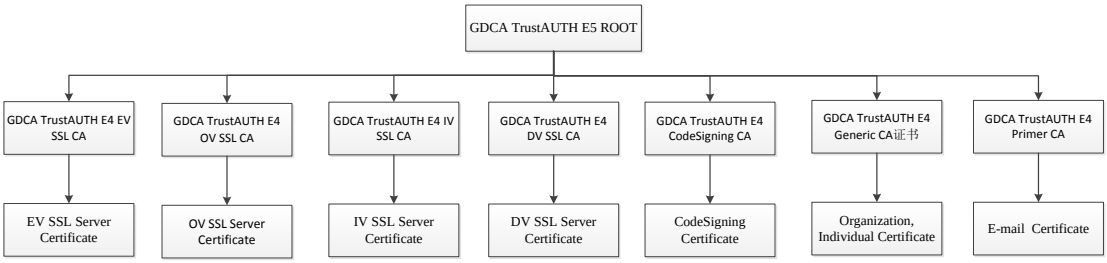
数安时代 R4 DV 服务器证书 CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

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

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 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 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 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 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 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 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 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 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 E5 ROOT certificate will expire on December 31, 2040.

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

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：GDCA 遵循 CA/B 论坛（https://www.cabforum.org.）发布的最新版本的 Baseline Requirements、EV Guidelines、Code Signing Baseline Requirements 、NCSSR、S/MIME Baseline Requirements 及 AATL 技术要求进行签发和管理公共可信任的 SSL/TLS 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 CPS，如果本 CPS 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 that 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, the EV Guidelines, the Code Signing Baseline Requirements of the CA/B Forum, the NCSSR, S/MIME Baseline Requirements, and the AATL Technical Requirements for the issuance and management of the publicly-trusted SSL/TLS digital certificates, 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 CPS according to these updates. The specifications of the CA/Browser Forum shall prevail in case of any discrepancies between the provisions of this CPS and the standard specifications published by the CA/Browser Forum.

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电子认证业务规则》（简称 GDCA CPS、本 CPS），CPS 为“Certification Practice Statement”的缩写。在本文档中，CPS 等同于本节中定义的文档名称和适用名称。有关本版本 CPS 的修订信息请参考附录 2。

本 CPS 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 called "GDCA Certification Practice Statement" (abbreviated as “GDCA CPS”, or “this CPS”). And CPS is equivalent to “GDCA CPS”. Please refer to Appendix 2 for detailed revisions of this version.

This document is the Chinese-English bilingual edition of GDCA CPS, 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

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、提供数字证书验证服务等手段而成为电子认证活动的参与主体。

GDCA is a trusted third-party electronic authentication service authority established by law pursuant to "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 engage in electronic transactions.

1.3.2. 注册机构 Registration Authorities

GDCA 的数字证书注册机构是经 GDCA 正式授权后的业务分支机构，包括证书注册审核（RA）中心、证书本地受理点（LRA）等。注册机构是为 GDCA 的证书申请者建立注册过程的实体。

Registration Authorities are branches authorized formally by GDCA, including Register Authority (RA), Local Registration Authority (LRA), etc. A Registration Authority is an entity that establishes registration process for certificate applicants.

1.3.3. 订户 Subscribers

在电子签名应用中，订户即是电子签名人或证书持有人，是 GDCA 颁发证书的最终用户，可以是个人、机构或基础设施的组成部件如路由器、防火墙、服务器或用于安全通信的其他设备。

In the application of electronic signature, subscribers also called electronic signers or certificate holders are end users of the certificates issued by GDCA. The subscribers could be the individual, organization or components of infrastructure such as router, firewall, server or other equipment used for secure communication.

1.3.4. 依赖方 Relying Parties

GDCA 的证书依赖方是指基于对 GDCA 提供电子认证活动中电子签名的信赖而从事有关活动的实体。该实体可以是，也可以不是 GDCA 的一个证书订户。

Relying Parties are the entities who are engaged in related electronic certification activities based on its trust of the electronic signatures provided by GDCA. This entity may, or may not be a certificate subscriber.

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. 适合的证书应用 Appropriate Certificate Usage

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、电子商务及其他社会化活动中，以实现身份认证、电子签名、关键数据加密等目的，同时也确保互联网上信息传递双方身份的合法性和真实性以及信息的完整性和保密性。

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 certificates 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 签发的证书，从功能上可以满足下列安全需要：

1. 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。
2. 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。
3. 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。
4. 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。

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

1. Authenticity of identity: the certification can ensure the validity of certificate holder using GDCA trust services.
2. Verification of integrity: the assurance to an entity that data has not been tampered and further verifies the consistency of information between sender and receiver using certificate of GDCA.
3. Confidentiality: the certification can ensure the confidentiality of information during transmission, and avoid the leakage to other non-authorized parties.
4. 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、

S/MIME 安全邮件类证书、SSL 服务器类证书、代码签名类证书等。其中：

- 对于个人类证书和机构类证书，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；
- 对于 S/MIME 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；
- 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；
- 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；
- 设备类证书、时间戳证书不再对其进行分类。

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

- 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;
- 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;
- 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;
- For CodeSigning Certificates, there are normal CodeSigning Certificates and EV CodeSigning Certificates;
- 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。

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.

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 证书和代码签名证书）：

There are four different types of individual certificate (Type I and Type II individual certificates are not applicable to SSL 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。第 1 类个人证书可以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。第 2 类个人证书可以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。第 3 类个人证书可以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。第 4 类个人证书可以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。第 3 类机构证书可以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。该级证书必须是以硬件介质为载体的证书，如 USB Key 或服务器密码机等，可以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. This type of certificates must be used with hardware medium, such as a USB Key or a cryptographic server. 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 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 server, firewall and router, etc. It is usually used for identification and secure communication among online facilities. For example, the browser can identify the server with certificate issued for the server to create SSL communication channel for secure communication 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 服务器证书标识 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 加密通道，不得用于各类交易、支付的签名或验证。

SSL server certificate is a digital certificate that identifies the website or server, applicable for verification of website certificates and provides SSL 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：

- EV SSL 证书（Extended Validation SSL Certificates），即扩展验证型服务器证书
- OV SSL 证书（Organization Validation Certificates），即需要验证网站所属机构真实身份的标准型 SSL 证书
- 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
- 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

SSL server certificates of GDCA include the following:

- EV SSL certificate (Extended Validation SSL Certificates), the extended validation SSL certificates.
- OV SSL certificate (Organization Validation Certificates), the SSL certificate requires to verify the identity of the organization that owns the website.
- IV SSL certificate (Individuals Validation SSL Certificates), the SSL certificate requires to verify the individual identity of website owner.
- 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 证书电子认证业务规则》，本 CPS 不再对其进行具体阐述。

SSL 服务器证书不限制域名的种类，如商业域名、政府域名等。

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 CPS”, which is no longer covered in this CPS.

The types of domain names in SSL 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。

代码签名证书订户必须承诺，不得将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。

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.

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

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

粤港互认个人证书策略对象标识符：2.16.156.339.1.1.1.2.1

粤港互认机构证书策略对象标识符：2.16.156.339.1.1.2.2.1

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)

Hong Kong-Guangdong mutual recognition individual certificates: 2.16.156.339.1.1.1.2.1

Hong Kong-Guangdong mutual recognition organization certificates: 2.16.156.339.1.1.2.2.1

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	1.2.156.112559.1.1.1.1	密钥用法：数字签名，密钥加密，数据加密。	2022 年 11 月 1 日起不再用于

1 类证书）		增强型密钥用法：客户端身份验证，电子邮件保护。	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 and key usages 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 2.23.140.1.5.1.2	KU: Digital Signature, Key Encipherment, Data 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

每一类型的证书，都只能应用于证书所代表的主体身份适合的用途。例如，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，机构证书不能作为个人和设备证书来使用，设备证书也不能作为个人和机构证书来使用。与应用类型不一致的证书，不应被本 CPS 识别为可信任。

Each certificate shall only be used to in dedicated usage corresponding to the subject's identity. For example, the Individual Certificate can only be used as individual case rather than the cases being used as Equipment or Organization Certificate; the Organization Certificate cannot be used as Individual and Equipment Certificate; the Equipment Certificate cannot be used as Individual or Organizational Certificate. Certificates shall not be deemed as trusted by this CPS 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订户自行承担。

The GDCA certificates are prohibited to be used in circumstances, such as any violation of state laws, regulations and national security or legal consequences, in addition, the GDCA certificates are 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 subscribers 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

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，负责审核批准 CPS。

The GDCA Security Policy Committee is the highest management authority for all policies related to GDCA's electronic certification services, responsible for reviewing and approving the Certification Practice Statement (CPS).

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

策略文档管理机构为 GDCA 安全策略委员会，作为策略管理机构负责制订、发布、

更新本 CPS。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。

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。

GDCA Security Policy Committee is assigned as the document management authority responsible for establishing, publishing and updating this CPS. 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.

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

任何有关 CPS 的问题、建议、疑问等，都可以按以下方式进行联系。

联系部门：GDCA 行政管理部门

联系人：王女士

网站地址：https://www.gdca.com.cn/

电子邮箱地址：gdca@gdca.com.cn

联系地址：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

邮政编码：510030

电话号码：+86 20-83487228

For any problems, suggestions, questions, etc., about this CPS, you could contact us as follow:

Contact Department: GDCA Administrative Department

Contact: Ms. Wang

Website: https://www.gdca.com.cn/

E-mail: gdca@gdca.com.cn

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

Postal Code: 510030

Tel: +86 20-83487228

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

GDCA 安全策略委员会决定 CPS 符合策略的机构。

The GDCA Security Policy Committee is the authority responsible for determining compliance of the CPS with applicable CP.

1.5.4. CPS 批准程序 CPS Approval Procedures

本机构的 CPS 由 GDCA 安全策略委员会组织 CPS 编写小组拟定文档，CPS 编写小组完成后提交 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，并根据《电子认证服务管理办法》的规定，从对外发布之日起的三十日之内向工业和信息化部备案。

This CPS is drafted by the team designated by GDCA Security Policy Committee. After the completion of drafting, the CPS is submitted to GDCA Security Policy Committee for review. After approval by the committee, GDCA will publish the CPS on its official website. Under the provisions of "Measures for the Administration of Electronic Certification Services", GDCA should put the record to the Ministry of Industry and Information Technology within 30 days after the publication.

1.5.5. CPS 修订 CPS Revision

GDCA 将对 CPS 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等及时修订本 CPS，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 CPS。

CPS 编写小组根据以上情况拟定 CPS 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 CPS 至少每年修订一次。如果无内容改动，则递增版本号、更新发布时间、生效时间及修订记录。

修订后的 CPS，从对外发布之日起三十日之内向工业和信息化部备案。

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

This CPS 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 CPS according to the latest versions of the Baseline Requirements, and the EV Guidelines, Code Signing Baseline Requirements, S/MIME Baseline Requirements and the NCSSR of the CA/B Forum (https://www.cabforum.org).

The proposed suggestion of revision will be submitted by the team which is responsible for writing CPS based on relevant changes, then it would be reviewed by the GDCA Security Policy Committee. After approved by the committee, GDCA will publish the updated CPS on its official website.

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

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

1.6. 定义和缩写 Definitions and Acronyms

1.6.1. 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 CPS 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。
录入员	负责录入证书申请者提交的信息，协助用户办理数字证书申请、撤销、更新等手续。
审核员	负责审核证书申请信息，并批准签发证书。
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 CPS 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 CPS 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.
Entry Clerk	Entry clerk is responsible for inputting the information submitted by the applicant and help the user handle certificates application, revocation and renewal procedures etc.
Reviewer	The reviewer is responsible for checking the information of certificate application and approving certificate issuance.
Fully Qualified Domain Name	A Domain Name that includes the labels of all superior nodes in the 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 CPS.
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. 信息发布与信息管理 Publication and Repository Responsibilities

2.1. GDCA 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，这些内容必须保持与 CPS 和有关法律法规一致。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 is 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 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。

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。

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 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 check the current status of certificate instantly via OCSP service provided by GDCA.

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撤销时，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）。

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

For 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.

GDCA can independently 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. 名称类型 Types of Names

GDCA 颁发的数字证书，含有颁发机构和证书订户主体甄别名，对证书申请者的身

份和其它属性进行鉴别，并以不同的标识记录其信息。证书持有者的标识命名，以甄别名（Distinguished Name）形式包含在证书主体内，是证书持有者的唯一识别名。GDCA 的证书符合 X.509 标准，分配给证书持有者实体的甄别名，采用 X.500 标准命名方式。

Certificate issued by GDCA can authenticate the identity and other attributes for applicant with different identifier including issuer and Distinguished Name (abbreviated as DN) of subscriber. The identifier of certificate holder is named as the DN contained in the certificate, and the DN is unique identifier of the subscriber. The certificate 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，所有的域名或 IP 地址都添加到主题别名中，而通用名为主域名或 IP 地址，必须是一个出现在主题别名中的域名或 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.

GDCA 证书颁发机构的主体甄别名命名规则如下：

Naming rules of issuer's DN are as follows:

属性	值
国家（C）	CN
省（S）	证书颁发者所在省份，或者不用
地区（L）	证书颁发者所在城市，或者不用
机构（O）	Global Digital Cybersecurity Authority Co., Ltd.或 GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.
机构部门（OU）	GDCA 可能依据用户类型、应用领域、区域的不同采用不同的颁发者为用户颁发证书，所以 GDCA 证书中可以包含不同的颁发者名称。
通用名（CN）	此属性为 CA 名

Attribute	Value
Country（C）	CN
State（S）	State of issuer (if included)
Local（L）	Local of issuer (if included)
Organization（O）	Global Digital Cybersecurity Authority CO.,LTD. or GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.

Organization Unit（OU）	Certificate contains various issuers depend on subscriber types, applications and regions to issue the certificate.
Common Name（CN）	Name of CA

GDCA 证书订户的主体甄别名命名规则如下：

Naming rules of subscriber's DN are as follows:

属性	值
国家（C）	CN
省（S）	订户所在省份，或者不用
地区（L）	订户所在城市，或者不用
机构（O）	对于有确定机构的订户，是订户所在机构名称；
机构部门（OU）	可以包含以下一个或多个内容： 订户所在机构的具体部门； 其他描述身份或证书类型的文字；
电子邮件（E）	订户的电子邮件地址，或不用
通用名（CN）	域名（SSL/TLS 证书），或机构名（机构类型证书），或个人姓名（个人类型证书），或其他可识别的名称

Attribute	Value
Country（C）	CN
State（S）	State of subscriber (if included)
Local（L）	Local of subscriber(if included)
Organization（O）	Organization where subscriber subordinates for certain one;
Organization Unit（OU）	One or more following options can be included: OU of subscriber subordinates; Any descriptions which describe identity or certificate type;
Email（E）	Subscriber's email address (if included)
Common Name（CN）	Domain name (SSL/TLS certificate), organization name (organization certificate), individual name (individual certificate), or other identifiable names

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

GDCA 使用 DN 项来标识证书主体及证书签发者实体，DN 项中的名称具有一定的代表性意义，可以与使用证书的最终实体的身份或特有的属性相关。证书主体名称标识本证书所提到的最终实体的特定名称。

GDCA uses the DN field to identify the entity that is the subject of the certificate and the entity that is the issuer of the certificate, and the names in the DN have representative meanings and can be related to the identities and specific properties of the final entities that use the certificates. The common name identifies the end entity's particular name mentioned by this certificate.

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

本 CPS 规定，GDCA 的订户在进行数字证书申请时不能使用匿名或伪名。

Under this CPS, subscriber cannot apply for certificate with anonymity or pseudonymity.

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

GDCA 签发的数字证书符合 X.509 V3 标准，甄别名格式遵守 X.500 标准。甄别名的命名规则由 GDCA 定义。

A certificate issued by GDCA conforms to X.509 V3. The format of DN conforms to X.500, and naming rules of DN are defined by GDCA.

3.1.5. 名称的唯一性 Uniqueness of Names

在 GDCA 信任域内，不同订户的证书的主体甄别名不能相同，必须是唯一的。但对于同一订户，GDCA 可以用其唯一的主体甄别名为其签发多张证书。当证书申请中出现不同订户存在相同名称时，遵循先申请者优先使用，后申请者增加附加识别信息予以区别的原则。

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

3.1.6. 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. Applicants can use the ways of digital signature contained in certificate request messages (PKCS#10) or other equivalent method to identify the private keys, or other ways required by GDCA, such as initial information (distributed key medium and its PIN code), etc. to prove that applicants hold the relevant keys.

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

对于个人身份证书，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。

For individual certificates, 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.

1. 对于第 1 类个人证书，执行以下鉴别：

   GDCA 只需验证用户所提交的信息，不对订户的身份进行验证。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。

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

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：

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。

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

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：

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。

2) 确认申请者的地址（如证书主题中包含地址）。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。

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。

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。

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。如查询第三方数据库、发送确认电子邮件等。

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

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 inspects 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) In case the subject of the certificate contains an address, 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) GDCA verifies the certificate request with the applicant by sending e-mails or making phone calls etc.

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) 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：

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。

2) 确认申请者的地址（如证书主题中包含地址）。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。

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。

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。

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。

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。如查询第三方数据库、发送确认电子邮件等。

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

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 inspects 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) In case the subject of the certificate contains an address, 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) GDCA verifies the certificate request with the applicant by sending e-mails or making phone calls etc.

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) 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.

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 an e-mail to the organization, etc.

5. 对于粤港跨境互认证书的个人身份鉴别：

当个人提出申请粤港跨境互认证书时，GDCA 采用以下方式之一进行鉴别：

1) 面对面鉴别。通过法定的身份证明文件（包括但不限于身份证、护照或者其它身份证明资料），确认个人的真实身份，并确保其身份与所申请的证书主体相对应。

2) 非面对面鉴别。GDCA 执行以下鉴别步骤：（1）个人提供身份证的拍照照片，GDCA 通过“粤港电子签名证书互认试点工作组”认可的独立权威第三方数据库（例如内地的“全国公民身份证号码查询服务中心”）进行比对，确认申请者的真实身份；（2）结合生物特征确认身份证与申请人的一致性（如脸部特征的比对）；（3）通过拍照、语音或视频确定个人申请证书的真实意愿；（4）通过第三方身份认证辅助信息源（例如内地 eID 或内地银行对外提供的个人账户和身份信息对应关系验证）验证申请人身份真实性，并与其签订身份鉴别的法律责任划分协议。

在合理情况下 GDCA 也会使用认为必须的其它额外鉴别方式或获取其他额外的材料。

5. For the individual mutual recognition certificate of Guangdong and Hong Kong, GDCA adopts one of the following ways to perform authentication:

1) Face to face authentication. GDCA confirms the authenticity of the individual identity by a legal identity document (including, but not limited to, identity cards, passports or other identification documents), and ensures the individual identity is consistent with subject information of the certificate requested.

2) Non face to face authentication. GDCA performs the following procedures for the authentication:

(1) Confirm the authenticity of the individual identity by comparing the photo taken of the ID document of the individual with an independent and authoritative third-party database (e.g. the National Citizen Identity Information Enquiry Service Center) recognized by the “Guangdong HongKong Electronic Signature Certificate Mutual Recognition Pilot Working Group”. (2) Confirm the consistency between the individual identity and the identity of the applicant using biometric characteristics (e.g. by comparing the facial features); (3) Confirm the willingness of the certificate request via voice communication, video communication, photo taking, etc. (4) Verify the authenticity of the applicant identity via a third party auxiliary data source on identity certification (e.g. using the services provided by eID and banks on mainland China designed to map relationship between the identities and personal accounts), and sign a legal responsibility agreement on identity authentication with the applicant.

If necessary, GDCA may also establish other reasonable authentication methods or obtain additional information.

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。

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。

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

The applicant is obliged to ensure the authenticity of the application materials and shall 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四类个人证书的鉴别要求执行。

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 建立评估标准用于识别存在潜在高风险欺诈情况的证书请求。对于识别为“高风险”的证书请求，GDCA 直接予以拒绝。

For the subscriber certificate issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA 证书 and GDCA TrustAUTHE5 ROOT, GDCA establishes evaluation process to identify the applicant with potential high risk. GDCA refuses the certification request from high-risk applicants.

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

任何组织机构（政府机构、企事业单位等），在以组织机构名义申请机构类证书时，应进行严格的身份鉴别，如通过查询可信数据库验证其真实性、面对面鉴别身份材料以及其他可以获得申请者明确的身份信息的方式等。机构类订户的证书申请表上有申请者本身或被充分授权的证书申请者代表的签字（公章）表示接受证书申请的有关条款，并承担相应的责任。

Identities of organizations (government agencies, enterprises and institutions, etc.), which apply for organization certificates, shall be authenticated strictly by cross-checking with the trusted databases, making a face to face validation and other ways that can clearly prove the identity of the subscriber, etc. Subscriber or subscriber's representative fully delegated by the organization should sign the application form with company's chop, and accept and affords corresponding responsibilities described in the subscriber agreement.

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. 第 3 类机构证书的机构身份鉴别

1) 确认机构是真实存在的、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。

2) GDCA 可以通过语音通话、视频、拍照等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。如有需要，GDCA 可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，以确认被申请者某个信息的真实性，如验证代理人的职位或验证申请表中的某个人是否是申请人。

3) 检查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，确保经办人得到申请机构的授权。

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

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) GDCA may verify the information provided by the subscriber through voice communication, video, photo taking, etc. If necessary, GDCA may contact the organization based on

information from third party, such as telephone number, email address and so onto verify the authenticity of the applicant's information, e.g. job position of representative or whether the person from the application form is the real applicant.

3) GDCA validates the materials submitted by the authorized agent and the identity of the agent to ensure the authorization.

2. 第 4 类机构证书的身份鉴别

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，并通过签发有效文件的权威第三方数据库进行核查确认。

2) GDCA 必须通过语音通话、视频、拍照等方式对申请者提供的信息进行确认（面对面鉴别时现场确认），并查询权威第三方数据库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，必要时，GDCA 还应执行面对面鉴别的方式。如有需要，GDCA 可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，以确认被申请者某个信息的真实性，如验证代理人的职位或验证申请表中的某个人是否是申请人。

3) 检查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，确保经办人得到申请机构的授权。必要时，应对授权代表人身份实施面对面的审核方式。

4) 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机构的身份，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。

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

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) GDCA must verify the information provided by the subscriber through voices communication, videos, photos taking, etc. (on-site verification for face to face cases) and also cross-checking with well-known third-party database, to ensure the consistency of the information from different channels. If necessary, GDCA may contact the organization based on information obtained from the third party, such as telephone number, email address and so on to verify the authenticity of a particular information item of the applicant, e.g. job position of representative or whether the person from the application form is the real applicant.

3) GDCA validates the materials submitted by the representative, as well as the identity of the representative and the signed document from the organization to verify the authorization from the organization. If necessary, GDCA shall do a face to face validation for the representative.

4) 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.

3. 粤港跨境互认证书的组织机构身份鉴别

当任何组织机构（政府机构、企事业单位或其它社会组织等）提出粤港跨境互认申请时，GDCA 应当先对其身份进行严格的鉴别，包括但不限于：

1） 由独立、权威的第三方提供的资料证明该组织确实存在，例如由政府机构发出的合法性证明，或由其它被认可的权威组织提供的证明资料；

2） 通过有效方式确认组织机构申请资料的真实性，确保申请已得到该组织机构充分的授权并能提供其它必须验证的信息；

3） 申请的组织机构证书包括个人身份名义时，GDCA 应要求该组织机构核实确认个人身份的真实性，并要求提交有关材料进行审核；

4） 申请的组织机构证书由授权代表申请时，GDCA 应要求授权代表提交该组织机构充分授权的书面证明文件（如授权书），审核确认授权代表得到该组织机构的明确授权；

5） 以面对面的审核方式确认授权代表身份,通过法定的身份证明文件（包括但不限于身份证、护照或者其它相关身份证明资料），确认授权代表的真实身份。

在采用以上审核方式的基础上，GDCA 还可以采用认为必要的其他额外鉴别方式和资料。

3. The organization mutual recognition certificate of Guangdong and Hong Kong

For the organization mutual recognition certificate of Guangdong and Hong Kong, the following authentication is performed:

When organizations (government agencies, enterprises and institutions, etc.) apply for organization mutual recognition certificate of Guangdong and Hong Kong, GDCA conducts a strict authentication process on its identity, including, but not limited to:

1) To confirm the existence of the organization through information (e.g. proof of legality issued by a government agency) provided by an independent, authoritative third party or supporting information provided by other recognized authoritative organizations.

2) Validate the authenticity of the organization's application materials in an efficient manner to ensure that the application has been fully authorized by the organization which can provide additional information that must be verified.

3) If the organization certificate includes the identity of the individual, GDCA shall request the organization to verify the authenticity of the individual identity and to submit relevant materials for review.

4) When an authorized representative applying for an organization certificate, GDCA shall request the representative to submit a written document (such as a letter of attorney) that is fully authorized by the organization, and to verify that the representative has been specifically authorized by the organization.

5) Conducting a face to face authentication on an identity of authorized representative, GDCA confirms the identity of the representative by a legal document of attestation (including, but not limited to, identity cards, passports or other identification documents).

On the basis of the above processes, GDCA may also adopt additional authentication methods and require extra data that it deems necessary.

此外，必要时，GDCA 还可以设定其它所需要的鉴别方式和资料。

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。

对于 Adobe 机构文档签名证书，其身份鉴别方式遵循本节第四类机构证书的鉴别要求执行。

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 建立评估标准用于识别存在潜在高风险欺诈情况的证书请求。对于识别为“高风险”的证书请求，GDCA 直接予以拒绝。

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

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

For the subscriber certificate issued by the subordinate CAs of GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA 证书 and GDCA TrustAUTHE5 ROOT, GDCA establishes evaluation process to identify the applicant with potential high risk. GDCA directly rejects the certification requests from such high risk applicants.

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别，包括如下内容：

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。

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

Subscriber submits application form of equipment certificate with original and copy of owner’s ID, authorization of operation 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 CPS 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 CPS 第 3.2.3 节第 4 类机构证书鉴别流程执行。

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。

核查授权经办人的有效身份。

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。

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

GDCA checks whether the key information submitted by the applicant complies with those from valid documents or information from third-party database in order to avoid the writing mistakes.

GDCA checks the authorized delegated person’s ID.

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。

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 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.

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 CPS 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 CPS 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：

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 CPS 第 3.2.3 节第 4 类机构证书鉴别流程执行。

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 CPS 第 3.2.2

节第 4 类个人证书鉴别流程执行。

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。

对于 EV SSL 证书，其鉴别方式遵循《GDCA EV 证书电子认证业务规则》，本 CPS 不再对其进行具体阐述。

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 CPS 第 3.2.9 节执行。

GDCA 不签发含有内部名称的 SSL 证书。

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

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 CPS.

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 CPS.

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

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

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 CPS section 3.2.9.

GDCA does not issue SSL certificates containing internal names.

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。

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 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.

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 CPS 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 CPS 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 证书电子认证业务规则》，本 CPS 不再对其进行具体阐述。

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。

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 CPS section 3.2.3; for individual subscriber, GDCA performs certificate validation process in accordance with the Type IV individual authentication in CPS section 3.2.2. The validation procedures of EV CodeSigning certificates is described in the GDCA EV CPS and not covered in this document.

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 CPS 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 CPS.

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

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 CPS 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 CPS 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 CPS. 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 CPS. 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 审核通配符右侧的域名，保证通配符（*）右侧的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 CPS 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 CPS.

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 CPS 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 CPS. 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 does 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，及更改或伪造的可抗性进行评估，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的时间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的时间不超过证书签发前 825 天，则 GDCA 可使用该数据及文件，对于根据本 CPS 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.

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 CPS, 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 CPS 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 CPS. 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 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 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 allows an applicant to specify individuals to request certificates. If an applicant specifies, in writing, the individuals who may request a certificate, then GDCA does not accept any certificate requests that are outside this specification. GDCA provides 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。

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。

截至目前，GDCA 未签发任何交叉证书。

如果国家法律法规对此有规定，GDCA 将严格予以执行。

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

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

To date, GDCA has not issued any cross certificates.

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

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 在执行多视角签发验证时，可以使用相同的一组或不同的一组网络视角，以完成以下两项必要检查：1）域名授权或控制，以及 2）CAA 记录检查。

来自所依赖网络视角集合的响应结果必须向 GDCA 提供必要的信息，以便其能够明确评估以下内容：

a. 存在符合预期的：1)随机值，2)请求令牌，3) IP 地址，或 4)联系地址。上述内容均应符合本 CPS 第 3.2.9 和 3.2.12 节中规定的验证方法要求；以及

b. GDCA 对所请求域名签发证书的授权有效性，如本 CPS 第 4.2.4 节所规定。

本 CPS 第 3.2.9 节和第 3.2.12 节描述了需要使用多视角签发验证的方法，以及网络视角如何对主网络视角所确定的结果进行佐证。

从一个网络视角获得的结果或信息不得在执行后续网络视角的验证过程中被重用或缓存（例如，不同的网络视角不得依赖共享的 DNS 缓存，以防止攻击者通过控制某一网络视角的流量来污染其他网络视角使用的 DNS 缓存）。为网络视角提供互联网连接的网络基础设施，可以由负责提供运行该网络视角所需计算服务的同一组织进行管理。所有远程网络视角与 GDCA 之间的通信必须通过依赖现代协议（例如 HTTPS）的经过身份验证且加密的通道进行。

网络视角可以使用未与其物理共址的递归 DNS 解析器。然而，该网络视角所使用的

DNS 解析器必须位于与其所属的网络视角相同的区域互联网注册管理机构服务区域内。此外，在一次多视角签发验证过程中使用的任意两个 DNS 解析器之间的直线距离必须至少为 500 公里。DNS 解析器的位置由其未封装的出站 DNS 查询首次交由提供该解析器互联网连接的网络基础设施的交接点确定。

GDCA 可立即重试多视角签发验证，并可使用相同的验证方法或替代方法（例如，如果“约定的网站变更”方法未能验证多视角签发验证的结果，GDCA 可以立即改用“发送电子邮件至 DNS TXT 联系地址”的方法重新进行验证）。在重试多视角签发验证时，GDCA 不得依赖先前尝试中的验证结果或佐证信息。对于在任意时间段内允许执行的验证尝试次数，没有具体限制。

“多视角验证一致性要求表”描述了与多视角签发验证相关的一致性数量要求。如果 GDCA 在进行域名授权或控制以及 CAA 记录检查时使用的网络视角集合不同，则两个集合（即域名授权/控制集合与 CAA 记录检查集合）均必须满足相应的一致性数量要求。当两个网络视角之间的直线距离至少为 500 公里时，它们被视为不同的。当一个网络视角与主网络视角及组成一致性数量的其他网络视角不同地点时，该网络视角被视为远程的。

GDCA 可以在最长 398 天内重复使用 CAA 记录一致性数量合规所需的佐证证据。在向某个域名签发证书后，远程网络视角在随后来自同一申请者的证书请求中，可以在最长 398 天内省略对该域名或其子域名的 CAA 记录重新检索和处理。

多视角验证一致性要求表

使用的不同远程网络视角数量	允许的不一致验证结果数量
2-5	1
6 及以上	2

执行多视角签发验证的远程网络视角应符合以下要求：

必须执行：

- 网络加固

依赖具备缓解全球互联网路由系统中 BGP 路由事件措施的网络（例如互联网服务提供商或云服务提供商网络）来提供网络连接。

应当执行：

- 设施与服务提供商要求
  - 部署于通过 ISO/IEC 27001 认证或具备同等安全框架、并已独立审计和认证或报告的设施。

- 所依赖的服务应包含以下报告之一：系统与组织控制报告 2（SOC 2）、IASE 3000、ENISA 715、FedRAMP Moderate、C5:2020、CSA STAR CCM，或其他经独立审计、认证或报告的等效服务框架。

- 漏洞检测与补丁管理
  - 实施入侵检测与防御控制措施，以防御常见的网络和系统威胁。
  - 建立并执行漏洞修复流程，包括漏洞的识别、审查、响应与修复。
  - 至少每三（3）个月进行一次漏洞扫描。
  - 至少每年进行一次渗透测试。
  - 在安全补丁发布后六（6）个月内应用推荐的安全补丁，除非 GDCA 记录证明该补丁会引入新的漏洞或系统不稳定，从而导致风险超过修补收益。
- 系统加固
  - 禁用所有未使用的账户、应用程序、服务、协议和端口。
  - 为所有用户账户实施多因素认证。
- 网络加固
  - 配置每个网络边界控制设备（防火墙、交换机、路由器、网关或其他网络控制系统），仅允许其运行所需的服务、协议、端口和通信。
  - 依赖的网络（如互联网服务提供商）应当：1）使用基于安全域间路由（RFC 6480）的机制，例如 BGP 前缀来源验证（RFC 6811）；2）使用其他非 RPKI 的路由泄露防护机制（如 RFC 9234）；3）遵循 BCP 194 中描述的当前最佳实践。建议在正常运行条件下，执行多视角签发验证的网络视角应通过过滤 RFC 6811 定义的 RPKI 无效 BGP 路由的网络或网络集合转发所有互联网流量，但这并非强制要求。

除上述要求外，执行多视角签发验证的计算系统被视为不在本 CPS 第 8 节所述的审计范围之内。

若上述措施由委托第三方执行，GDCA 可以从该委托第三方获取合理证据，以确认其遵循了一项或多项相关要求。作为对本 CPS 第 1.3.2 节的例外，为满足上述要求，委托第三方无需纳入本 CPS 第 8 节所规定的审计范围。

分阶段实施时间表：

自 2024 年 9 月 15 日起：

GDCA 应当使用至少两个（2）远程网络视角实施多视角签发验证。

自 2025 年 3 月 15 日起：

GDCA 必须使用至少两个（2）远程网络视角实施多视角签发验证。若不符合“多视角验证一致性要求表”中规定的允许不一致数量（即远程网络视角未能验证主网络视角结论的数量超出允许范围），GDCA 可以继续签发证书。

自 2025 年 9 月 15 日起：

GDCA 必须使用至少两个（2）远程网络视角实施多视角签发验证。GDCA 必须确保满足“多视角验证一致性要求表”中定义的要求。若未满足这些要求，GDCA 不得继续签发证书。

自 2026 年 3 月 15 日起：

GDCA 必须使用至少三个（3）远程网络视角实施多视角签发验证。GDCA 必须确保满足“多视角验证一致性要求表”中定义的要求，且与主网络视角结果一致的远程网络视角必须分布于至少两个（2）不同的区域互联网注册管理机构服务区域内。若未满足上述要求，GDCA 不得签发证书。

自 2026 年 6 月 15 日起：

GDCA 必须使用至少四个（4）远程网络视角实施多视角签发验证。GDCA 必须确保满足“多视角验证一致性要求表”中的要求，且验证结果与主网络视角一致的远程网络视角分布于至少两个不同的 RIR 服务区域。若未满足上述要求，GDCA 不得签发证书。

自 2026 年 12 月 15 日起：

GDCA 必须使用至少五个（5）远程网络视角实施多视角签发验证。GDCA 必须确保满足“多视角验证一致性要求表”中的要求，且与主网络视角验证结果一致的远程网络视角分布于至少两个不同的 RIR 服务区域。若未满足上述要求，GDCA 不得签发证书。

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 may use either the same set, or different sets of network perspectives when performing Multi-Perspective Issuance Corroboration for the required 1) domain authorization or control and 2) CAA record checks.

The set of responses from the relied upon network perspectives shall provide GDCA with the necessary information to allow it to affirmatively assess:

a. the presence of the expected 1) Random Value, 2) Request Token, 3) IP Address, or 4) Contact Address, as required by the relied upon validation method specified in sections 3.2.9 and 3.2.12 of this CPS; and

b. GDCA's authority to issue to the requested domain(s), as specified in section 4.2.4 of this CPS.

Sections 3.2.9 and 3.2.12 of this CPS describe the validation methods that require the use of Multi-Perspective Issuance Corroboration and how a network perspective can corroborate the outcomes determined by the primary network perspective.

Results or information obtained from one network perspective shall not be reused or cached when performing validation through subsequent network perspectives (e.g., different network perspectives cannot rely on a shared DNS cache to prevent an adversary with control of traffic from one network perspective from poisoning the DNS cache used by other network perspectives). The network infrastructure providing Internet connectivity to a network perspective may be administered by the same organization providing the computational services required to operate the network perspective. All communications between a remote network perspective and GDCA shall take place over an authenticated and encrypted channel relying on modern protocols (e.g., over HTTPS).

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

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

The "Quorum Requirements" Table describes quorum requirements related to Multi- Perspective Issuance Corroboration. If GDCA does not rely on the same set of network perspectives for both Domain Authorization or Control and CAA Record checks, the quorum requirements shall be met for both sets of network perspectives (i.e., the Domain Authorization or Control set and the CAA record check set). Network perspectives are considered distinct when the straight-line distance between them is at least 500 km. Network perspectives are considered "remote" when they are distinct from the primary network perspective and the other network perspectives represented in a quorum.

GDCA may reuse corroborating evidence for CAA record quorum compliance for a maximum of 398 days. After issuing a certificate to a domain, remote network perspectives may omit retrieving and processing CAA records for the same domain or its subdomains in subsequent certificate requests from the same applicant for up to a maximum of 398 days.

Quorum Requirements Table

Distinct Remote Network Perspectives Used	**Allowed non-Corroborations**
2-5	1

6+	2

Remote network perspectives performing Multi-Perspective Issuance Corroboration:

MUST:

- Network Hardening
  - Rely upon networks (e.g., Internet Service Providers or Cloud Provider Networks) implementing measures to mitigate BGP routing incidents in the global Internet routing system for providing internet connectivity to the network perspective.

SHOULD:

- Facility & Service Provider Requirements
  - Be hosted from an ISO/IEC 27001 certified facility or equivalent security framework independently audited and certified or reported.
  - Rely on services covered in one of the following reports: System and Organization Controls 2 (SOC 2), IASE 3000, ENISA 715, FedRAMP Moderate, C5:2020, CSA STAR CCM, or equivalent services framework independently audited and certified or reported.
- Vulnerability Detection and Patch Management
  - Implement intrusion detection and prevention controls to protect against common network and system threats.
  - Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities.
  - Undergo or perform a Vulnerability Scan at least every three (3) months.
  - Undergo a Penetration Test on at least an annual basis.
  - Apply recommended security patches within six (6) months of the security patch's availability, unless GDCA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.
- System Hardening
  - Disable all accounts, applications, services, protocols, and ports that are not used.
  - Implement multi-factor authentication for all user accounts.
- Network Hardening
  - Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications identified as necessary to its operations.
  - Rely upon networks (e.g., Internet Service Providers) that: 1) use mechanisms based on Secure Inter-Domain Routing (RFC 6480), for example, BGP Prefix Origin Validation (RFC 6811), 2) make use of other non-RPKI route-leak prevention mechanisms (such as RFC 9234), and 3) apply current best practices described in BCP 194. While it is

recommended that under normal operating conditions Network Perspectives performing Multi-Perspective Issuance Corroboration forward all Internet traffic via a network or set of networks that filter RPKI-invalid BGP routes as defined by RFC 6811, it is not required.

Beyond the above considerations, computing systems performing Multi-Perspective Issuance Corroboration are considered outside of the audit scope described in section 8 of this CPS.

If any of the above considerations are performed by a delegated third party, GDCA may obtain reasonable evidence from the delegated third party to ascertain assurance that one or more of the above considerations are followed. As an exception to section 1.3.2, delegated third parties are not required to be within the audit scope described in section 8 of this CPS to satisfy the above considerations.

Phased Implementation Timeline:

- **Effective September 15, 2024**, GDCA should implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives.
- **Effective March 15, 2025**, GDCA shall implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. GDCA may proceed with certificate issuance if the number of remote Network Perspectives that do not corroborate the determinations made by the Primary Network Perspective ("non-corroborations") is greater than allowed in the Quorum Requirements table.
- **Effective September 15, 2025**, GDCA shall implement Multi- Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. GDCA shall ensure that the requirements defined in Quorum Requirements Table are satisfied. If the requirements are not satisfied, GDCA shall not proceed with issuance of the certificate.
- **Effective March 15, 2026,** GDCA shall implement Multi-Perspective Issuance Corroboration using at least three (3) remote Network Perspectives. GDCA shall ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then GDCA shall not proceed with issuance of the certificate.
- **Effective June 15, 2026**, GDCA shall implement Multi-Perspective Issuance Corroboration using at least four (4) remote Network Perspectives. GDCA shall ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then GDCA shall not proceed with issuance of the certificate.
- **Effective December 15, 2026**, GDCA shall implement Multi-Perspective Issuance Corroboration using at least five (5) remote Network Perspectives. GDCA shall ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then GDCA shall not proceed with issuance of the certificate.

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

在订户证书到期前，订户需要获得新的证书以保持证书使用的连续性。GDCA 一般要求订户产生一个新的密钥对代替过期的密钥对，称作“密钥更新”。

Prior to the expiration of an existing subscriber's certificate, it is necessary for the subscriber to obtain a new certificate to maintain continuity of certificate usage. In general, GDCA requires subscriber to generate the new key pair to replace the old one, which is called re-key.

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

对于一般正常情况下的更新密钥申请，订户须提交能够识别原证书的足够信息，如订户甄别名、证书序列号等，对申请的鉴别基于以下几个方面：

- 申请对应的原证书存在并且由认证机构签发；
- 用原证书上的订户公钥对申请的签名进行验证；
- 基于原注册信息进行身份鉴别。

For general application of rekey, subscriber must submit sufficient information for identifying original certificate, such as DN of subscriber, serial number of certificates, etc. Authentications are including the following:

- Original certificate issued by GDCA exists.
- GDCA verifies the signature of re-key request using subscriber’s public key in original certificate.
- GDCA authenticates the identity based on original registration information.

密钥更新会造成使用原密钥对加密的文件或数据无法解密，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 incurred by failure of decryption by the renewal of the secret key.

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

GDCA 不提供证书被撤销后的密钥更新。

GDCA does not provide Re-key/renewal after revocation.

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

当 GDCA 或注册机构有本 CPS4.9.1.1 所述理由需要撤销订户的证书时，有权依法撤销证书，这种情况无须进行鉴别。如果订户主动要求撤销证书，则按照本 CPS 第 3.2 节描述进行身份鉴别。

GDCA or RA can revoke a certificate based on reasons stated in section 4.9.1.1 of this CPS without authentication. Subscribers who request to revoke certificate follows CPS section 3.2.

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 CPS $3.2 的要求执行身份鉴别。承担 RA 职责的人员须满足本 CPS $5.3.1 的要求。同时授权 RA 应根据本 CPS $ 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 CPS. Relevant personnel undertaking the RA duties must meet the requirements of section 5.3.1 of this CPS. In the meantime, the authorized RA must archive relevant documentation and records as required by section 5.5.2 of this CPS.

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

自 CA 认证系统签发之日算起，GDCA 签发的个人类型证书、机构类型证书的有效期一般为 3 年或以内，最长不超过 5 年；时间戳服务器证书的有效期为 5 年或以内；设备类型数字证书的有效期为 10 年或以内；SSL/TLS 服务器证书的有效期为 398 天或以内，代码签名证书的有效期为 39 个月以内，S/MIME 安全邮件证书的有效期为 825 天或以内。一个完整的证书生命周期包括申请、验证、签发、发布、更新、挂起、撤销、

归档等过程。

From the issuance date by GDCA system, individual and organization certificates are generally valid for a period no more than 3 years, with a maximum validity not exceeding 5 years; time stamp server certificates are valid for a period no more than 5 years; equipment certificates are valid for a period no more than 10 years; SSL/TLS server certificates are valid for no more than 398 days, and CodeSigning certificates are valid for a period no more than 39 months, S/MIME certificates are valid for no more than 825 days. A whole certificate life cycle includes the application, verification, issuance, distribution, renewal, logout, revocation and archiving, etc.

4.1. 证书申请 Certificate Application

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

证书申请实体包括个人和具有独立法人资格的组织机构(包括国家机关、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 government agencies, public institutions, social organizations, people's organizations and other organizations).

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

1. 证书的注册过程

1) 订户填写相应的证书申请表单。

2) 订户将相应的申请材料提交给 GDCA 的注册机构（RA 或 LRA）进行证书申请，注册机构审核通过后，录入申请资料。其中审核员和录入员分别为两个不同的系统操作人员。

3) 注册机构向 GDCA 提交证书请求，通过应用安全协议发送至 GDCA。

4) GDCA 根据注册机构的请求签发证书。

5) 注册机构通过安全的方式将证书交付给订户。

2. 责任

1) 申请者应事先了解订户协议、CP 及本 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。

2) 订户有责任向 GDCA 提供真实、完整和准确的证书申请信息和资料。

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

1. Certificates registration process

1) Subscribers shall fill in the certificate application forms.

2) Subscribers shall submit the corresponding application materials to the registration authorities, i.e. RA or LRA of GDCA, for the application. After reviewed by RA, the request data are recorded. The reviewer and entry clerk are two different system operators respectively.

3) The certificate requests submitted by RA shall send to GDCA through the secure channel**.**

4) GDCA issues certificates according to the registered agencies' requests.

5) RAs deliver certificates to the subscribers in a secure way.

2. Responsibilities

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

2) The subscriber has the responsibility to provide real, complete and accurate certificate application information to GDCA.

3) 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. 识别与鉴别功能 Performing Identification and Authentication Functions

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

GDCA 在处理证书申请过程中，将通过有效手段确保证书信息与正确的申请信息相符，并将证书签发给正确的申请者。

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 CPS 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 CPS 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 CPS 3.2.

In the process of certificates application, GDCA will take effective measures to ensure that the certificate information is in line with correct application information, and the certificate is issued to the right applicant.

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 CPS) 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 CPS) 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

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

GDCA 注册机构成功完成了证书申请所有必需的确认步骤并提交证书请求后，GDCA 通过发行正式证书来批准证书申请。

After GDCA's registration authority successfully completes verification steps for the certificate application and submits a certificate request, when GDCA formally issues certificates, it means GDCA has approved the certificate application.

如果符合下述条件，注册机构（RA）可以批准证书申请：

1. 该申请完全满足本 CPS 3.2 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 CPS 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，注册机构（RA）拒绝证书申请：

1) 该申请不符合本 CPS 3.2 关于订户身份的标识和鉴别规定；
2) 申请者不能提供所需要的身份证明材料；
3) 申请者反对或者不能接受订户协议的有关内容和要求；
4) 申请者没有或者不能够按照规定支付相应的费用；
5) 申请的证书含有 ICANN（The Internet Corporation for Assigned Names and Numbers）考虑中的新 gTLD（顶级域名）；
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。

If the following circumstances happened, GDCA refuses the certificate application in case of the following situations:

1) The application does not meet the specifications of subscriber's identification and authentication in CPS 3.2.
2) The applicant cannot provide the required identity documents.
3) The applicant opposes or does not accept the relevant content or requirements of the subscriber's agreement.
4) The applicant has not paid or cannot pay the appropriate fees.
5) The requested certificates contain a new gTLD under consideration by ICANN (The Internet Corporation for Assigned Names and Numbers).
6) GDCA or RA considers that the approval of the application will bring about controversies, legal disputes or losses to 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 授权的注册机构将做出合理努力来尽快确认证书申请信息，一旦注册机构收到了所有必须的相关信息，将在 2 个工作日内处理证书申请。

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

RA authorized by GDCA will make a reasonable effort to check the certificate application information as soon as possible. Once RA received all the necessary information, it will process the certificate application within 2 working days.

The capability of the RA to process the applications within the period mentioned above will depend on whether the applicant has submitted the true, complete and accurate information as well as responded the management requirement of GDCA in time.

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 要求的公共可信任的 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 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 processes "issue", "issuewild", and “iodef” property tags according to RFC8659: GDCA will 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 will determine whether or not to issue certificates after communicating with the applicant.

GDCA treats 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 CPS 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 CPS.

4.3. 证书签发 Certificate Issuance

4.3.1. 证书签发过程中注册机构（RA）和电子认证服务机构（CA）的行为 CA Actions During Certificate Issuance

根 CA 的证书签发由 GDCA 授权的至少 2 名可信人员参与，其中一人谨慎地发布直接指令，使根 CA 执行证书签名操作。

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。

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。

GDCA 在批准证书申请之后，将签发证书。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

通常 GDCA 签发的证书在 24 小时内生效。

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。

At least two trusted persons authorized by GDCA are required in order for the root CA to perform a certificate signing operation, one of whom deliberately issues a direct command with respect to certificate issuance by the root CA.

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.

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

GDCA will issue the certificate after approval over certificate application. The issuance of the certificate means GDCA approves the certificate request formally.

In general, certificates issued by GDCA will take effect within 24 hours.

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

GDCA 会采取以下几种通告方式告知订户：

1、电子或纸质的受理回执；

2、电子邮件（e-mail）；

3、通过面对面的方式，通知订户（如申请者到受理点领取等方式）；

4、其他 GDCA 认为安全可行的方式。

GDCA will take the following notification ways to inform subscribers:

1. Electronic or paper receipt
2. E-mail
3. Face to face (such as the applicant gets certificate from LRA, etc.)
4. Other secure and practical manners considered by GDCA

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数字证书载体中，证书下载完毕即代表订户接受了证书。
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。
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。

4. 订户反对证书或者证书内容的操作失败。

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. 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. Subscribers have received the way of obtaining the certificates, and no objection of the certificates or their contents.
4. Subscribers failed to oppose or conduct the operation of objection over the certificates or the content of certificates.

对于 GDCA TrustAUTH R4 OV SSL CA 及 GDCA TrustAUTH R4 CodeSigning CA 证书签发的订户证书，构成接受证书的行为：

1. 订户自行访问专门的 GDCA 证书服务网站将证书下载，证书下载完毕即代表订户接受了证书。
2. GDCA 注册机构在订户的允许下，代替订户下载证书，并把证书通过邮件及其他 GDCA 认为可靠方式发送给订户，即代表订户接受了证书。
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。
4. 订户反对证书或者证书内容的操作失败。

For subscriber certificates issued by GDCA TrustAUTH R4 OV SSL CA and GDCA TrustAUTH R4 CodeSigning CA Certificate, the following behaviors constitute acceptance of certificate:

1. Subscribers access to specialized GDCA certificate service website and download the certificate. When the certificate is completely downloaded, it represents that the subscriber have received a certificate.
2. GDCA's RA downloads certificate on behalf of the subscribers, when a subscriber receives a certificate from RA through e-mail represents that the subscriber has received the certificate.
3. Subscribers have received the way of obtaining the certificates, and no objection of the certificates or their contents.
4. Subscribers fail to oppose or conduct the operation of objection over the certificates or the content of certificates.

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

订户接受证书后，GDCA 在 24 小时内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。

GDCA 采用主、从目录服务器结构来分布所签发证书。签发完成的数据直接发布到主目录服务器中，然后通过主从映射，将主目录服务器的数据自动同步到从目录服务器中，供订户和依赖方查询和下载。

After a subscriber receives a certificate, GDCA issues the subscriber certificate to the GDCA directory service system within 24 hours. 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.

GDCA uses the main and subordinate directory server architecture to distribute issued certificates. Issued data are directly released to the main directory server, and then through the master-slave mapping, the main directory server data automatically synchronized to the subordinate directory server for subscriber and relying party to query and download.

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

GDCA 及注册机构将不对其他实体进行通告。其他实体可以通过从目录服务器中查询到 GDCA 已经签发的数字证书。

GDCA and RA will not notice to other entities. Other entities can obtain GDCA's issued certificates by querying the directory server.

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

4.5.1. 订户的私钥和证书的使用 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 CPS 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 CPS 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 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：

1. 获得数字签名对应的证书及信任链；
2. 确认该签名对应的证书是依赖方信任的证书；
3. 通过查询 CRL 或 OCSP 确认该签名对应的证书是否被撤销；
4. 证书的用途适用于对应的签名；
5. 使用证书上的公钥验证签名；
6. 检查证书的有效期。

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. Obtain digital signature's corresponding certificate and trust chain.
2. Confirm that the signature's corresponding certificate is the one trusted by the relying party.
3. Confirm whether the signature corresponding certificate has been revoked by querying the CRL or OCSP.
4. Certificate usage is suitable for the corresponding signature.
5. Use certificate's public key to verify the signature.
6. Check the validity of the certificates.

以上条件不满足的话，依赖方有责任拒绝签名信息。

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。

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

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。

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，更新时无需再提交证书注册信息，订户提交能够识别原证书的足够信息，如订户甄别名、证书序列号等，使用原证书的私钥对包含公钥的更新申请信息签名。

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，更新申请要求和流程与初次申请时一样。GDCA 根据 Baseline Requirements 的要求确认是否重用此前已验证的信息：若在证书更新前，GDCA 根据 CPS 3.2 指定来源获得的数据或证明文件的时间不超过 825 天（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。

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

For the subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, when renewing a certificate, the subscriber no longer needs to submit certificate registration information, instead, he/she only needs submit sufficient information which can identify the original certificate, such as subscriber DN, certificate serial number, etc. using the private key of the original certificate to sign for the renewal application information containing of the public key.

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 requirements and procedures for renewing the certificates are the same with those for the initial certificates request. GDCA confirms

whether or not to use the previously validated information according to the Baseline Requirements: GDCA may use the documents and data provided in section 3.2 to verify certificate information, provided that it obtained the data or document from a source specified under section 3.2 no more than 825 days prior to renewing 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.

4.6.1. 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 subscibers 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. 证书更新请求的处理 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：

1. 订户的原证书存在并且由 GDCA 所签发；
2. 验证证书更新请求在许可期限内；
3. 基于原注册信息进行身份鉴别。

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. The original certificate of subscribers exist and issued by GDCA
2. Validate the certificate update request is in validity period.
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。

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

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

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.

- 订户对申请信息进行签名，CA 用其原有证书中的公钥对签名进行验证
- 订户注册信息没有发生变化，CA 基于其原有注册信息对其进行签发新的证书
- Subscriber signs off the application information, and CA verifies signature by the original certification's public key.
- There is no change on subscriber's registration information, and CA issues a new certificate based on their original registration information accordingly.

订户也可以选择一般的初始证书申请流程进行证书更新，按照本 CPS 第 3.2 节的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。

Subscribers can also choose the initial certificate application process to apply for the certificate update, and submit the application and identification information required based on CPS 3.2. In any cases, the identification of initial certificate application process will be used for the method of certificate update.

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

同本 CPS 第 4.3.2 节。

See CPS 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 CPS 第 4.4.1 节。

See CPS Section 4.4.1.

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

同本 CPS 第 4.4.2 节。

See CPS Section 4.4.2.

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

同本 CPS 第 4.4.3 节。

See CPS Section4.4.3.

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。

证书密钥更新时无需再提交证书注册信息，订户提交能够识别原证书的足够信息，

如订户甄别名、证书序列号、原证书对应的私钥对证书密钥更新请求签名等，并上送新的公钥申请签发新证书。

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.

When the certificate key is updated, the subscriber has no need to submit the registration certificate, while can only submit sufficient information that can identify the original certificate, such as subscriber's DN, certificate serial number, the certificate key renewal signature of the original certificate's corresponding private key, and send a new public key for applying a new certificate.

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：

1. 证书私钥泄露而撤销证书。
2. 证书到期。
3. 基于技术、政策安全原因，GDCA 要求证书密钥更新。

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

1. Revocation certificate due to private key leakage.
2. The certificate expires.
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. 证书密钥更新请求的处理 Processing Certificate Rekeying Requests

GDCA 对证书密钥更新请求的处理通过证书更新请求处理流程完成。

GDCA 证书密钥更新请求的处理流程同本 CPS 第 4.6.3 节描述。

The process of certificate key update request is completed by the process of certificate update request in GDCA.

The process of GDCA certificate key update request is described as CPS section 4.6.3.

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

同本 CPS 第 4.3.2 节。

See CPS 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 CPS 第 4.4.1 节。

See CPS Section 4.4.1.

4.7.6. 电子认证服务机构对密钥更新证书的发布 Publication of the Rekeyed Certificate by the CA

订户接受证书后，GDCA 在其规定的时间内将该订户更新后的证书发布到 GDCA 的目录服务系统。

After subscribers receive a certificate, GDCA will issue the subscriber updated certificate to the GDCA directory service system in the specified time.

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

同本 CPS 第 4.4.3 节。

See CPS Section 4.4.3.

4.8. 证书变更 Certificate Modification

当证书信息发生变化时，订户须重新办理证书。GDCA 不予接受对已发出的证书的内容做出变更的请求。

When there are some changes over the certificate information, subscriber shall apply for the certificate again. GDCA will not accept the request of modification on the certificates which are already issued.

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。

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。

证书变更的申请和证书申请所需的流程、条件是一致的。

If the registered information which subscriber provide has some changes, the subscriber has to submit the certificate modification to GDCA.

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.

Both the procedures and conditions of the certificate application and modification are 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. 证书变更请求的处理 Processing Certificate Modification Requests

证书变更按照初次申请证书的注册过程进行处理。

The certificate modification is processed following the registration procedures where the first application for a certificate.

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

同本 CPS 第 4.3.2 节。

See CPS 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 CPS 第 4.4.1 节。

See CPS Section 4.4.1

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

订户接受证书后，GDCA 在其规定的时间内将该订户证书发布到 GDCA 的目录服务系统。

After subscribers accept a certificate, GDCA will issue the subscriber certificate to the GDCA directory service system in the specified time.

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

同本 CPS 第 4.4.3 节。

See CPS 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 节的相关要求；

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; or
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;
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. GDCA 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 terminated.
2. The private key of the certificate has been compromised or is suspicious of being compromised.
3. The management consideration.

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 GDCA 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. 在任何 GDCA 得知证书中的域名或 IP 地址的使用不再被法律所允许的情形，如域名注册者使用域名的权利已被法院或仲裁机构撤销、与域名注册机构的合约终止、

域名注册者更新域名失败等；

2. GDCA 得知一个通配符证书被用来验证一个欺诈性误导的子域名；
3. GDCA 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. GDCA 签发证书的权利已届满或被撤销或终止，除非 GDCA 已做出安排，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 compromised, 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 needs to revoke the certificates:

1. The situation which of GDCA knew domain name or IP address in the certificate no longer allowed been used by law, e.g. the right of registrar's domain name has been canceled from court or arbitration organization; or fail to renew the domain name 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 risks 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

请求证书撤销实体为订户、注册机构、GDCA、经司法机构授权的司法人员。此外，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 subscribers, RA, GDCA, or judicial officials authorized by judicial institutions can initiate revocation. Additionally, 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.

4.9.3. 撤销请求的流程 Procedure for Revocation Request

4.9.3.1. 订户主动提出撤销申请 The subscriber actively proposed to revocation application.

1. 订户向注册机构提出证书撤销申请，注册机构核实申请撤销实体的身份和授权实体的身份。
2. 注册机构将证书撤销申请表提交给 GDCA，由 GDCA 完成撤销。

3. GDCA 提供 7*24 小时的证书撤销申请服务，订户可通过以下方式申请撤销：
   - E-mail: webtrustreport@gdca.com.cn
   - 电话号码：4007008088

   GDCA 收到申请后 24 小时内处理撤销申请。

1. Subscribers may submit the revocation request to the RA and the RA will verify the identity of subscriber and the delegated party.
2. RA submits a revocation application form to GDCA and GDCA completes the revocation operation.
3. GDCA offers 24x7 certificate revocation requests service, and subscribers may request the revocation of a certificate through the following ways:
   - E-mail to: webtrustreport@gdca.com.cn
   - Call: 4007008088

GDCA will process the revocation requests within 24 hours after receiving.

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

1. 当 GDCA 或注册机构有本 CPS4.9.1.1 所述理由需要撤销订户的证书时，GDCA 或注册机构的有关人员可以通过内部确定的流程提请撤销证书。
2. 在证书撤销后，GDCA 或注册机构将通过适当的方式，包括邮件、电话等，通知最终订户证书已被撤销及被撤销的理由。若未能联络订户时，在必要的情况下，GDCA 对撤销的证书将通过网站进行公告。
3. GDCA 提供 7*24 小时的证书问题报告和处理流程。
4. 当依赖方、司法机构、应用软件提供商、防病毒机构等第三方发现证书可能存在问题，如私钥出现或怀疑出现泄漏、证书滥用、证书被用于可疑代码签名等，可及时通过以下方式进行问题报告：
   - E-mail: webtrustreport@gdca.com.cn
   - 电话号码：4007008088

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

   （1） 所报告问题的性质；

   （2） 相应问题的出现次数和频率；

   （3） 问题报告或投诉的实体；

   （4） 用户对 GDCA CP/CPS 和订户协议等相关规范的遵循情况；

（5） 现行法律法规的遵循。

1. When the GDCA or RA has a reason stated in section 4.9.1.1 of this CPS to revoke a subscriber certificate, related person of GDCA or RA can revoke the certificate through internal formalized process.
2. After the certificate revocation, GDCA or RA will use appropriate ways, including mail, phone, fax to notify the final subscriber that the certificate has been revoked and the reason why to be revoked. If we cannot contact subscriber, if necessary, GDCA will publish the information of the revoked certificate on its official website.
3. GDCA maintains a 24x7 certificate problems reporting and processing procedures.
4. The relying parties, judicial institutions, application software providers, anti-virus organizations and other third parties may contact GDCA timely through the following ways in case they found any suspicious problems in relation to the certificates, such as private key disclosure or suspicious disclosure, certificates abuse, the use of certificates to sign suspicious codes etc.

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

GDCA will investigate the reported problems of certain certificates within 24 hours of receipt, and will decide whether or not to revoke the certificates based on the following criteria:

(1) The nature of the alleged problem;

(2) The number and frequency of certain certificate problem reports received;

(3) The entity making the reports or complaints;

(4) Subscribers' compliance with the GDCA CP/CPS, the Subscriber Agreement, and other relevant specifications;

(5) Compliance with existing laws and regulations.

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

对于 GDCA 的根证书和中级证书，GDCA 根据本 CPS 的规定决定是否撤销证书。对于由国家密码管理局签发给 GDCA 的中级 CA 证书，必须经过国家密码管理局确定并执行撤销。

For GDCA's Root CA certificates and Subordinate CA certificates, revocation will be determined according to this CPS. For the subordinate CA certificate issued by a Root CA of OSCCA, revocation must be determined and performed by OSCCA.

4.9.4. 撤销请求宽限期 Revocation Request Grace Period

如果出现密钥泄露或有泄露嫌疑等事件，撤销要求必须在发现泄密或有泄密嫌疑 8 小时以内提出。其他撤销原因的撤销要求必须在变更前的 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 in within 48 hours.

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

GDCA 处理撤销请求的周期为 24 小时。

The cycle of GDCA processes revocation request is 24 hours.

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

GDCA 提供在线撤销状态查询，依赖方可在 GDCA 的网站上进行查询。

GDCA provides online query on revocation status. The relying party can query on the GDCA website.

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 updates and publishes certificate revocation list (CRL) every 12 months. In case the subordinate CA certificates are revoked, GDCA updates and publishes the certificate revocation list (CRL) within 24 hours after the revocation, and the value of the nextUpdate field is not 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

GDCA 的 CRL 发布最大滞后时间为发布周期之后的 24 小时内。

Maximum latency for GDCA's CRLs is 24 hours after release cycle.

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

GDCA 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 RFC6960 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 服务器的证书包含一个 RFC6960 定义的类型为 id-pkix-ocsp-nocheck 的扩展项。

GDCA supports OCSP responses for subscribers and the relying parties. The OCSP responses conform to RFC6960, 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 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 没有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 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 至少每 12 个月更新 OCSP 信息。当撤销中级 CA 证书

时，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 不返回“good”状态。

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

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

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

GDCA does 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

GDCA 不提供撤销信息的其他发布形式。

Currently GDCA does not provide other forms of announcement about the revoked certificates.

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

除本 CPS 第 4.9.1 节规定的情形外，当订户或注册机构的证书密钥已经失密或者可能已经失密时，必须及时向 GDCA 提出证书撤销请求。

Except for the case described in CPS Section 4.9.1, when certificate key of subscriber or RA has been or may have been lost, certificate revocation request must be made to GDCA immediately.

证书订户以外的第三方可根据本 CPS 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

不适用。

Not applicable.

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

不适用。

Not applicable.

4.9.15. 挂起请求的流程 Procedure for Suspension Request

不适用。

Not applicable.

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

不适用。

Not applicable.

4.10. 证书状态服务 Certificate Status Services

4.10.1. 操作特征 Operational Characteristics

订户可以通过 CRL、LDAP、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 在证书到期前不删除其在 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 服务器中的撤销记录。

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

For the revoked certificates, GDCA does 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 responder.

4.10.2. 服务可用性 Service Availability

GDCA 提供 7*24 小时的证书状态查询服务，且响应时间不超过 10 秒。即在网络允许的情况下，订户能够实时获得证书状态查询服务。

GDCA provides 7X24 certificate status query services, and the response time is of ten seconds or less. If the network is permitted, the subscriber can timely obtain certificate status query services.

4.10.3. 可选特征 Operational Features

证书状态的其他可选服务方式为订户利用 GDCA 指定的 CRL 地址，通过目录服务器提供的查询系统，查询并下载 CRL 到本地，进行证书状态的查询。

Other optional service of certificate status for subscriber is using CRL address which is specified by GDCA. The subscriber can query and download CRL to query certificate status locally through query system provided by the directory server.

4.11. 订购结束 End of Subscription

订购结束包含以下情况：

1. 当订户停止使用 GDCA 提供的数字证书时，必须向 GDCA 提出证书撤销的申请。申请流程为本 CPS 第 4.9.3 节的规定。GDCA 撤销证书后，表明订户的订购行为正式结束。
2. 当证书有效期结束后，订户未按时续缴服务费时，表明订户的订购行为正式结束。
3. 证书有效期期满，没有进行证书更新或密钥更新，表示订户订购行为正式结束。

The following conditions shall be deemed that the user terminated the use of the certificate services provided by GDCA:

1. When the subscriber stops using certificate provided by GDCA, an application of certificate

cancellation must be made to GDCA. The application process is described as CPS Section 4.9.3. After GDCA revokes the certificate, it indicates that the subscriber's ordering behavior has been formally terminated.

2. After the expiration of the certificate, if the subscriber doesn't pay the renewal service fee, this indicates that the subscriber's ordering behavior has been formally terminated.

3. After the expiration of the certificate, if the subscriber has not carried out certificate or key update, it indicates that the subscriber's ordering behavior has been formally terminated.

一旦用户在证书有效期内终止使用 GDCA 的证书认证服务，GDCA 在批准其终止请求后，将实时把该订户的证书撤销，并按照 CRL 发布策略进行发布；GDCA 详细记录撤销证书的操作过程并定期将订购结束后的证书及相应订户数据进行归档。

Once the user terminates the use of GDCA certificate authentication services within the certificate validity period, GDCA will revoke the certificate in real time after approves on his or her request for termination, and release in accordance with the CRL distribution strategy. GDCA will record the process of revoking certificates in details and archive the certificates whose subscription is over and the corresponding subscriber's data regularly.

4.12. 密钥生成、备份与恢复

Key Escrow and Recovery

4.12.1. 密钥生成、备份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：

GDCA 要求订户必须使用本订户的数字证书载体生成签名密钥对。订户可以委托 GDCA 代订户进行生成签名密钥对的有关操作。由于签名私钥遗失所造成的损失由订户自己承担，GDCA 对此不承担责任。

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，可以向 GDCA 提出申请恢复加密密钥，GDCA 按照流程，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:

GDCA requires subscribers to generate signature key pairs by their own certificate carriers.

Subscribers can authorize GDCA to generate signature key pairs and other related operations. 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.

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和行为 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 的建筑物和机房建设按照下列标准实施：

The GDCA's building and data center shall be constructed in accordance with the following standards:

- GB/T 25056-2018 《信息安全技术 证书认证系统密码及其相关安全技术规范》
- GM/T0054-2018 《信息系统密码应用基本要求》
- GB50174 《电子信息系统机房设计规范》
- SJ/T10796-1996 《计算机机房用活动地板技术条件》
- GB2887-2011 《计算机场地通用规范》
- GB30003 《电子计算机机房施工及验收规范》
- GB50222 《建筑内部装修设计防火规范》
- GB50116 《火灾自动报警系统设计规范》
- GB50057 《建筑物防雷设计规范》
- GB5054 《低压配电设计规范》
- GB/J19 《采暖通风与空气调节设计规范》
- SJ/T10796 《计算机机房用活动地板技术条件》
- GB/T 25056-2018 "Information security techniques- Specifications of cryptograph and the related security technology for certificate authentication system".
- GM/T0054-2018 "General Requirements for Information System Cryptography Application".
- GB50174 "Code for design of electronic information System Room".
- SJ/T10796-1996 "Specification for raised floor of computer room".
- GB2887-2011 "Specification for computer field"
- GB30003 "Construction and acceptance test code for electronic computer room".
- GB50222 "Code for Fire Prevention in Design of Interior Decoration of Buildings".
- GB50116 "Code for design of automatic fire alarm system"

- GB50057 “Design code for protection of Structures against lightning”
- GB5054 “Code for design of low voltage electrical installations”
- GB/J19 “Code for design Of heating ventilation and air conditioning”
- SJ/T10796 “Specification for raised floor of computer rooms”

GDCA 机房位于佛山市南海区狮山镇，是一幢独立的建筑物，具备防震、防火、防水、防雷等功能，进入机房建筑区只有唯一的入口和道路，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。只有经过授权的人员才能进入授权的区域。

The data center of GDCA is an independent building located in Shishan Town, Nanhai District, Foshan City, Guangdong Province. The basic protection of GDCA’s data center include: shock-proof, fire-proof, water-proof, lighting-proof, etc., and with only one entrance and a single road. According to the functions, GDCA data center divided into core area, service area, management area, operation area, and public area. Only the personnel officially authorized by GDCA could access the restricted areas.

5.1.1.1. 公共区域 Public Area

公共区包括入口、大堂、保安室，部署各配套设施和监控设备。

Public area includes the entrance, lobby, security room and etc., deployed with various supporting facilities and monitoring devices.

5.1.1.2. 操作区 Operation Area

操作区是 RA 操作人员、管理人员的工作区，需要使用双因素身份认证才可以进入，人员进出操作区要有日志记录。从该层开始，所有的墙体都应采用高强度防护墙。

Operation area is a working place for RA operators and administrators. Anyone who wants to enter the operation area needs to use two-factor authentication. Every access behavior to the operation area has been well recorded. From this level of areas, all the walls are strengthened by high strength protective wall.

5.1.1.3. 管理区 Management Area

管理区安装 RA 管理控制台，CA 管理、签发、审计控制台，网络管理、监控控制台，是 RA 和 CA 管理员、审计员和网络安全员的工作区，只允许管理区规定的管理人员进入，需要两个管理员同时使用双因素身份认证才可以进入。

Management area is a working area for RA and CA administrators, auditors and network security

officers, installed with the RA management console, CA consoles of management, issue, and audit, and consoles of network management and monitor. Only authorized and specified administrators have the rights to access this area. Enter this area requires two administrators to use two-factor authentication.

5.1.1.4. 服务区 Service Area

服务区主要安装从 LDAP 服务器、OCSP 服务器、RA 注册服务器等设备；只允许服务区规定的管理人员进入，需要两个管理员同时使用双因素身份认证才可以进入。

Service area is installed with LDAP servers, OCSP servers, RA register servers and other related devices. Only authorized and specified administrators have the rights to access this area. Entering this area requires two administrators to use two-factor authentication.

5.1.1.5. 核心区 Core Area

核心区为屏蔽区，加装高强度的钢制防盗门，主要安装 CA 签名服务器、CA 数据库服务器、KM 密钥管理服务器、时间戳服务器等核心设备，只允许核心区规定的管理人员进入，而且需要两个管理员同时使用双因素身份认证才可以进入。密码柜也安放在核心区，存放保密资料。

Core area, a shielding zone with high strength steel security doors, is mainly installed with CA signature servers, CA database servers, KM key management servers, timestamp servers and other core devices. Only authorized and specified administrators have the rights to access this area. Entering this area requires two administrators to use two-factor authentication. The password ark for storing confidential information is also placed in the core area.

5.1.2. 物理访问 Physical Access

GDCA 机房内设有 9 扇门安装电子门禁系统和 1 个物理侵入报警器，对门禁系统进行监控，实时读取门禁记录的资料，并对门禁系统设置权限。该系统能实时读取进出门资料，并有门开超时报警。工作人员都需使用身份识别卡或结合指纹才能进出，并且进出每一道门都有时间记录和相关信息提示，服务区与核心区需要两个管理员同时使用身份识别卡和指纹鉴别才可以进入，机房工作人员按照机房日常工作规范，每月对门禁记录进行整理归档，保留一年的门禁记录。

In the data center of GDCA, it has 9 doors installed with electronic access systems and one physical intrusion alarm. The electronic access systems are monitored, with real-time access records to set permissions of access, and can set an alarm when the doors are opened over time. The staff is required to use the identity card and fingerprint to open every door, and each access

behavior has been recorded with time-stamp and related notice. Enter the service area and core area, two administrators need to use ID cards and fingerprint identification at the same time before entering the room. According to daily working specification, the specific personnel will archive the access records on a monthly basis, and retained for one year at least.

物理访问控制包括如下几个方面：

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

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

c) 监控系统：与门禁和物理侵入报警系统配合使用的还有录像监控系统，对安全区域和操作区域进行 7*24 小时不间断录像。所有录像资料至少保留 6 个月，以备查询。

Physical access controls includes the following aspects:

a) Access control system: It is used to control access to the doors on each floor. Staff needs to use identity card with a password or fingerprint to enter and exit. Entering or exiting every door should have the time records and related notice.

b) Alarm system: Alarm system will be triggered by any illegal intrusion, unauthorized opening, long time opening and other abnormal situations. Alarm system can clearly identify the alarm location.

c) Monitoring system: video monitoring system is working with access control systems and physical intrusion alarm system. The monitoring system is responsible for continuous recording the restricted area and operation area within 7*24 hours. All video records will be retained for at least 6 months in order to future inquiry.

5.1.3. 安防监控 Security Monitoring

根据机房动力环境保安监控系统的要求，本机房环境监控系统包括的子系统有：配电检测子系统、UPS 检测子系统、空调设备检测子系统、新风机检测子系统、温湿度检测子系统、漏水监测子系统、消防子系统、门禁子系统、图像监控子系统。对基础设施设备、机房环境状况、安防系统状况进行 7*24 小时实时监测，为满足故障诊断、事后审计的需要，监控记录保留时间为 6 个月以上。

According to the requirement of data center power and environment security monitoring system, it includes electronic detection subsystem, UPS detection subsystem, air conditioning equipment detection subsystem, fresh air machine detection subsystem, temperature and humidity detection subsystems, water leakage monitoring subsystem, fire control subsystem, access control subsystem and image monitoring subsystem. The system carries out real-time monitoring of infrastructure equipment status, data center environment condition and the security system status within 7*24 hours. In order to meet the need of fault diagnosis and post audit, monitor records will

be retained for more than 6 months.

5.1.4. 电力与空调 Power and Air Conditioning

本机房采用两路市电电源供电、一台柴油发电机，配置有专门的配电机房，每个机房配置有独立的配电设备、接地防雷系统。机房内采用了不间断供电系统 UPS，可提供大于 8 小时的电力。机房区域内采用了防静电措施，实现机柜、服务器、网络设备等电位连接和接地。

The data center uses dual power sources and a diesel generator for supplying electricity, and has a specialized electronic distribution room. The GDCA data center is equipped with independent power distribution equipment and the lightning-proof system. The data center area is supported by uninterruptible power supply which can provide more than 8 hours extra power. The data center area also takes anti-static to protect cabinets, servers and network devices.

机房的空调采用风冷式冷凝器机组，室外风冷式冷凝器机组放置在顶楼。机房按照 300kcal/h ṁ2 热负荷计算。夏季室外设计温度：35℃；冬季室外设计温度：0℃；机房室内设计温度：22±1℃，相对湿度：55±5%/h 。同时，机房安置了新风系统，对机房进行换气，保证机房内的空气品质和解决新风供应以及机房对空气清洁度的要求等问题。

The data center's air conditioning adopts air cooled condenser unit. The air cooled condenser unit is placed in the attic outside of the data center. According to 300kcal/h * M2 heat load, outdoor designed temperature is 35 Celsius degrees in summer and 0 Celsius degrees in winter. Indoor designed temperature is 22 +_ 1 Celsius degrees and relative humidity is 55 + 5%/h. Meanwhile, the data center is installed with a fresh air system for ventilation to ensure air quality inside and solve the problems of fresh air supply to meet the demands of specified air cleanliness, etc.

5.1.5. 水患防治 Water Exposures

为防治水害对机房的威胁，GDCA 在机房的空调室内设置漏水报警系统。漏水报警检测绳在空调周围设置，一旦发生水患立即报警，通知有关人员采取应急措施。同时在沿外墙四周做排水沟及泄水地漏，一旦发生水患，水能立即排泄出去，并对所有外窗已做封闭处理。

In order to protect the data center from water disasters, GDCA set water leakage alarm system inside the air conditioner room of data center. Once the flood is detected by detection ropes surrounding the air conditioners, the system will alarm immediately and notify related personnel to take emergency measures. At the same time, the data center is installed with a drainage ditch and a drainage floor along the periphery of the wall. Once the flood has occurred, water can be drained immediately, and all exterior windows are sealed.

5.1.6. 火灾防护 Fire Prevention and Protection

GDCA 机房内各区域均采用了烟感和温感火灾探测器，并安装了火灾自动报警系统及气体自动灭火系统，该系统具有自动、手动及机械应急操作三种启动方式。

在自动状态下，当防护区发生火警时，火灾报警控制器接到防护区两个独立火灾报警信号后立即发出联动信号。经过 30 秒时间延时，火灾报警控制输出信号，启动灭火系统，同时，报警控制器接收压力讯号器反馈信号，防护区内门灯显亮，避免人员误入。

The data center of GDCA uses smoke and temperature fire detectors in each area, and installs the fire automatic alarm and gas extinguishing system. The system has three operation modes including automatic, manual and mechanical emergency.

In the automatic mode, when protection district is on fire and detected by two independent alarms, fire alarm controller will immediately trigger a linkage signal. After 30 seconds' delay, the fire extinguishing system will be turned on. At the same time, alarm controller receives feedback signal from the pressure signal device, and the door light will be on in protection area in order to avoid personnel strayed.

当防护区经常有人工作时，可以通过防护区门外的手动/自动转换开关，使系统自动状态转换到手状态，当防护区发生火警时，报警控制器只发出报警信号，不输出动作信号。由值班人员确认火警，按下控制面板或击碎防护区外紧急启动按钮，即可立即启动系统，喷发气体灭火剂。

当自动、手动紧急启动都失灵时，可进入储瓶间内实现机械应急操作启动。

When the staffs work in the protection area, the automatic/manual switch outside the door in the protection area can be used to turn the system from automatic into manual. When the protection area is on fire, the alarm controller only sends the alarm signal and waits for operator to confirm, operator can press the control panel or shatter emergency start button in protection area to activate the system by using gas fire extinguishing agent.

When automatic and manual modes both fail, operator can activate mechanical emergency operation in the ampoule storage room.

5.1.7. 介质存储 Media Storage

GDCA 对物理介质的存放和使用满足防火、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。采取了介质使用登记注册、介质防复制及信息加密等措施实现了对介质的安全保护。

GDCA meets the following physical media storage and use security requirements: fire-proof, water-proof, shock-proof, moisture-proof, corrosion-proof, pest-proof, static-proof, electromagnetic radiation-proof, etc. and implement media usage registration, media copy protection, information

Confidentiality and other measures to achieve the security protection of the media.

5.1.8. 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 shall 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 will be initialized and physically destroyed by using manufacturer's method before disposal.

5.1.9. 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。这些角色包括但不限于：密钥和密码设备的管理人员、系统管理人员、安全审计人员、业务管理人员及业务操作人员等，具体岗位名称和要求以 GDCA 的岗位说明为准。

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 but are not limited to: key and cryptographic equipment administrators, system administrators, security audit administrators, business administrators and business operators, etc. The specific job names and requirements shall be subject to the GDCA job descriptions.

5.2.2. 每项任务需要的角色 Number of Persons Required per Task

GDCA 在具体业务规范中对关键任务进行严格控制，敏感操作需要多个可信角色共

同完成，例如：

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

GDCA strictly defines the controls of core missions in specific standards. Multiple trusted roles shall be required to jointly complete the sensitive operation. For example:

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

GDCA 所有承担可信角色的在职人员都应经过一定程序的鉴证。鉴证程序在 GDCA 的人员聘用管理条例中规定。

All current staff who undertakes the trusted roles in GDCA should pass certain accreditation process. This process is set out in the GDCA personnel management regulations.

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

为保证系统安全，遵循可信角色分离的原则，即 GDCA 的可信角色由不同的人担任。GDCA 进行职责分离的角色，包括但不限于下列角色：

a）证书业务受理

b）证书或 CRL 签发

c）系统工程与维护

d） CA 密钥管理

e）安全审计

In order to ensure security of the systems, it should follow the trusted role segregation principle that the trusted role must be assumed by different personnel in GDCA. Roles requiring segregation of duties include but are not limited to：

a) The acceptance of the certificate businesses

b) The issuance of certificates or CRLs

c) System Engineering and Maintenance

d) CA key management

e) Security auditing

5.3. 人员控制 Personnel Controls

5.3.1. 资格、经历和无过失要求 Qualifications, Experience, and Clearance Requirements

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和良好的从业经历。
5. 具备良好的团队合作精神。
6. 无违法犯罪记录。
7. 关键和核心岗位的工作人员必须具备相关的工作经验，或通过 GDCA 相关的培训和考核后方能上岗。

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.
7. Staff in key and core positions must have related working experience, or pass GDCA's related training and examination before they start their work.

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. 背景审查程序 Background Check Procedures

GDCA 或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。

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。背景调查必须符合法律法规的要求，调查内容、调查方式和从事调查的人员不得有违反法律法规的行为。背景调查应使用合法手段，尽可能地通过相关组织、部门进行人员背景信息的核实。

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

All employees who are trusted or apply for shall have a written consent that they must go through a background investigation. The background investigation complies with laws and regulations. The content and method of the investigation, officer engaging in the investigation shall not violate the laws and regulations. The background investigation will be conducted legally, in which background information of employees will be checked through the organization concerned.

背景调查分为：基本调查和全面调查。

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。

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。

Background review including: basic review and full review.

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

Full review includes reviewing criminal records, social relations and social security apart from 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)在背景调查中，对发现以下情形的人员，可以直接拒绝其成为可信人员的资格：

- 存在捏造事实或资料的行为；
- 借助不可靠人员的证明；
- 使用非法的身份证明或者学历、任职资格证明；
- 工作中有严重不诚实的行为。

d) 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。根据考察的结果做出相应的安排。

e) 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) In the background investigation, if GDCA finds the following circumstances, GDCA can directly refuse qualifications of trusted personnel:

- There is fabricating facts or information
- With evidence of the unreliable staff
- Use illegal identification or education, qualifications
- The behavior of serious dishonesty in the work

d) The HR department checks candidates through on-site assessment, daily observation, situational test and other methods. Appropriate arrangement is made according to the investigation result.

e) 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

GDCA 根据可信角色的职位需求，给予相应的岗前培训，综合培训内容如下：

- GDCA 运营体系；
- GDCA 技术体系；
- GDCA 安全管理策略和机制；
- 岗位职责统一要求；
- PKI 基础知识；
- 身份验证和审核策略和程序；

- 灾难恢复和业务连续性管理；
- CP、CPS 政策及相关标准和程序；
- GDCA 管理政策、制度及办法等；
- 国家关于电子认证服务的法律、法规及标准、程序；
- 其他需要进行的培训等。

Based on the requirements of trusted role, GDCA gives the corresponding pre-job training. The comprehensive training contents are as follows:

- GDCA operation system
- GDCA technology system
- GDCA security management strategy and mechanism
- Job responsibilities requirements
- PKI basic knowledge
- Authentication and the policies and procedures of audit
- Disaster recovery and business continuity management
- CP、CPS and related standards and procedures
- GDCA management policies, systems, measures, etc.
- The laws, regulations, standards and procedures of electronic certification service in China.
- Other needs of training

GDCA 将员工参加培训的情况形成记录并存档，对于签发 SSL/TLS 服务器证书和代码签名证书的操作员和审核员，上岗前必须通过培训并达到 Baseline Requirement 中要求的从事该项工作所必须的技能水平。

GDCA keeps a record about the participation in the training. The operator and assessor who issues SSL/TLS server certificates and Code Signing certificates must pass the training and reach the skill level required by Baseline Requirement which engaged in this work before starting the work.

5.3.4. 再培训周期和要求 Retraining Frequency and Requirements

对于充当可信角色或其他重要角色的人员，每年必须至少接受 GDCA 组织的培训一次。对于认证系统运营相关的人员，每年至少进行一次相关技能和知识培训。此外，GDCA 将根据机构系统升级、策略调整等要求，不定期的要求人员进行继续培训。

For persons acting as trusted roles or other important roles, they shall be trained at least once a year by GDCA. Related personnel for operating authentication system should have the training of

relevant skills and knowledge at least once a year. In addition, GDCA will provide ongoing training for employees irregularly according to system upgrade, strategy adjustment and other requirements.

5.3.5. 工作岗位轮换周期和顺序 Job Rotation Frequency and Sequence

GDCA 在职人员的工作岗位轮换周期和顺序将依据本机构的安全管理策略而制定。

GDCA will define and change the Job rotation cycle and the sequence based on the organization security management strategy.

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

当出现在职人员未经授权或超出权限使用 GDCA 系统、操作认证业务等情况时，GDCA 一经确认，将立即撤销该人员的登录证书、同时终止其系统访问权限，并视该人员未授权行为的情节严重性，实施对该名人员的通报批评、罚款、辞退以及提交司法机构处理等措施。

When the circumstances that in-service staff use GDCA systems, perform authorization businesses without or beyond the permission, once the above circumstances are confirmed by GDCA, we will immediately revoke the login certificates and simultaneously terminate the system access authorization. GDCA makes the implementation of the official notice criticism, fine, dismissal and submit judicial institutions and other measures depend on the seriousness of unauthorized behavior.

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、管理人员等独立签约者，GDCA 的统一要求如下：

- 人员档案的备案管理；
- GDCA 提供统一的岗前培训辅导和再培训要求，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:

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

5.3.8. 提供员工的文档 Documentation supplied to Personnel

在培训或再培训期间，GDCA 提供给员工的培训文档包括但不限于以下几类：

- GDCA 员工手册；
- GDCA 证书策略、电子认证业务规则和有关的协议和规范；
- GDCA 技术体系文档；
- GDCA 岗位职责说明书；
- 内部操作文件，包括业务连续性管理和灾难恢复方案等；
- GDCA 安全管理制度等。

During the training or retraining, GDCA provides training materials including but not limited to the following categories:

- GDCA employee handbook
- GDCA CP, CPS and related agreements and standards
- GDCA technology system documents
- GDCA job descriptions
- Internal operating files, including business continuous management, disaster recovery programs, etc.
- GDCA security management regulations

5.4. 审计日志程序 Audit Logging Procedures

5.4.1. 记录事件的类型 Types of Event recorded

所有发生在 GDCA 的重大安全事件会记录在审计跟踪档案中，可在必要时供合格审计师查看。这些记录，不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

这些事件包括但不限于：

1. 密钥生命周期内的管理事件，包括密钥生成、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. 信息安全设备记录的安全事件：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. CA 设施的访问，包括授权人员进出 CA 设施、非授权人员进出 CA 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 lifecycle, 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, including 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. 处理日志的周期 Frequency of Processing Log

GDCA 每月进行一次日志跟踪处理，检查违反政策及其它重大事件，每季度对发证系统进行日志分析。所有的审计日志定期由专人进行检查和审阅，以便发现重要的安全和操作事件，及时采取相应的措施进行处理。

GDCA carries out log tracking process on monthly a basis, reviews the violations of policies and other major events, and analyses the certificate issuance system logs on a quarterly basis. All the audit logs are checked and reviewed by specific personnel regularly in order to discover the significant security and operation events and take corresponding measures timely.

5.4.3. 审计日志的保存期限 Retention Period for Audit Log

GDCA 妥善保存电子认证服务的审计日志，在数据库保存审计日志至少两个月，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 retaining period of audit logs in database is at least two months. 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

GDCA 的审计日志储存在数据库里，并且实现备份，其中包括有关文档中的审计信息和事件记录。GDCA 执行严格的物理和逻辑访问控制措施，以确保只有授权人员才能接近这些审查记录，严禁未授权的访问、阅读、修改和删除等操作。

GDCA audit logs are stored in the database with backup, including audit information and event records in related documents. GDCA carries out strictly the measures of physical and logical access control to ensure that only personnel authorized by GDCA can be access to the records being reviewed. These records are strictly protected from unauthorized access, reading, modification and deletion.

5.4.5. 审计日志备份程序 Audit Log Backup Procedures

GDCA 的审计跟踪文档由运维人员和审计人员每月进行审计日志和审计文档的归档备份。所有文档包括最新的审计跟踪文档应储存在磁盘中并存放在安全的文档库内。

GDCA's audit tracking documents are carried out by the operation and maintenance team and auditor for the archiving of audit log and audit documents monthly. All documents including the latest audit tracking documents should be stored in secure disks and stored in a secure document library.

5.4.6. 审计收集系统 Audit Collection System

GDCA 的审计日志收集系统涉及：

1. 证书管理系统；
2. 证书签发系统；
3. 证书目录系统；
4. 远程通信系统；
5. 证书受理系统；
6. 访问控制系统；
7. 网站、数据库安全管理系统；
8. 其他需要审计的系统。

The GDCA Audit log collection system involves in:

1. Certificate management system
2. Certificate issuing system
3. Certificate directory system
4. Remote communication system
5. Certificate accepted and approval system
6. Access and control systems
7. Security system of website, database
8. Other systems considered by GDCA for necessary audit.

GDCA 使用审计工具满足对上述系统审计的各项要求。

GDCA uses the audit tools to meet the requirements of the system audit described above.

5.4.7. 对导致事件实体的通告 Notification to Event-Causing Subject

GDCA 发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

GDCA 有权决定是否对导致事件的实体进行通告。

When GDCA detects the attack attempts, it will record the behaviors of the attackers and try to track the attackers within the laws. And GDCA reserves the right to take appropriate countermeasures. According to the attacker's behavior, GDCA takes actions including cutting off the open services for attackers, submitting the evidences to jurisdiction and etc.

Whether to notify the attackers or the perpetrators is decided by GDCA.

5.4.8. 脆弱性评估 Vulnerability Assessments

CA 安全程序根据政策、技术和管理的变化、重大变更及时进行薄弱环节分析，属于可以弥补的薄弱环节，及时弥补，属于不可弥补的薄弱环节，GDCA 每年对系统进行脆弱性评估，以降低系统运行的风险。

CA security program carries out timely weakness analysis according to the changes in policies, in technology and management, and other major changes. The weaknesses should be remedied immediately. If some weaknesses can’t be remedied, GDCA will launch system vulnerability assessment each year in order to reduce the risks of system operation.

5.5. 记录归档 Records Archival

5.5.1. 归档记录的类型 Types of Records Archived

GDCA 对以下几类事件进行归档记录，包括但不限于：

1. 证书系统建设和升级文档；
2. 证书和证书撤销列表；
3. 证书申请支持文档，证书服务批准和拒绝的信息，与证书订户的协议；
4. 审计记录；
5. 证书策略、电子认证业务规则文档；
6. 员工资料，包括但不限于背景调查、录用、培训等资料；
7. 各类外部、内部评估文档。

GDCA archives the following events, including but not limited to:

1. Certificate system constructed and upgraded documents.
2. Certificate and certificate revocation list.
3. Certificate application for information, information about approval and rejection of certificate service, the certificate subscriber agreement.
4. Audit record
5. Certificate Policies and Certification Practice Statements.
6. Employee information, including but not limited to background investigation, hiring, training, etc.
7. Various external, internal documents of the review and assessment.

5.5.2. 归档记录的保存期限 Retention Period for Archive

对于不同的归档记录，其保留期限是不同的。对于系统操作事件和系统安全事件记录，其归档应保留到完成安全脆弱性评估或一致性审计。

1. 对订户证书生命周期内的管理事件的归档，保留不少于证书失效后 5 年。
2. 对 CA 证书和密钥生命周期内的管理事件的归档，其保留期限不少于 CA 证书和密钥生命周期。
3. 订户证书的归档保留期限不少于证书失效后 5 年。
4. CA 证书和密钥的归档在 CA 证书和密钥生命周期之外，额外保留 10 年。

For different archived records, the retention periods are different. For system operation event records and system security event records, the archives will be retained to complete the security vulnerability assessment or audit consistency.

1. Archiving for management events in subscriber certificate life cycle will be kept for no less than 5 years after the expiration of certificates.
2. Archiving for management events in CA Certificate and key life cycle will be kept for not less than life cycle of CA certificate and key.
3. Archiving retention period of subscriber certificates will not be less than 5 years after the expiration of certificates.
4. CA key and certificate archiving will be kept for 10 more years after the end of life cycle.

5.5.3. 归档文件的保护 Protection of Archive

审计跟踪文档的保护在以下章节中作详细说明。其中档案介质采用物理安全方式进行保护，并且保留一个严格限制的入口，只有 GDCA 的业务管理人员可以访问。

Protection of audit tracking documents will be illustrated in detail in the following sections. The archived media is protected by physical security way and set an entrance with restrict authorizations, and only business administrators of GDCA have the right of access.

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，每周进行备份，备份文件进行异地存放。

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。

所有归档的电子文件和数据库除了保存在 GDCA 的存储库，还在异地保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。GDCA 在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

Electronically archived records generated by the systems will be backed up weekly. The backup file will also be stored off-site.

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.

All the documents and data archived usually are stored in the main storage site of GDCA. If necessary, the backups will also be saved in the offsite. Archived database is generally isolated physically or logically, with no interaction with the outside. Only authorized personnel or others under the supervision can conduct the operation for reading the files. GDCA provide mechanisms to protect archives and backups from being deleted or modified.

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 Archives Collection System

GDCA 的审计跟踪档案收集系统在本 CPS 第 5.4 节中作详细说明。

分离媒体数据存储和该媒体安全存储的归档不属于 GDCA 系统。

GDCA audit trail collection system is detailed in section 5.4 of this CPS.

Storage of separated media data storage and archiving of its security storage are not included in GDCA 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 GDCA 归档信息的 2 个拷贝。在获得完整归档信息时，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's archived information respectively. While obtaining the complete archived information, comparison of the 2 copies shall take place to confirm the integrity.

5.6. 电子认证服务机构密钥的更替 Key Changeover

在证书到期以前，GDCA 将按照证书策略的规定对根密钥进行更换，生成新的证书。在进行密钥的生成时，严格按照 GDCA 关于密钥管理的规范。CA 密钥更替必须遵循以下原则：

1. 在 CA 证书生命周期结束前停止签发新的下级证书，确保在 CA 的证书到期时所有下级证书也全部到期。
2. 在停止签发新的下级证书后至证书到期时，继续使用 CA 私钥签发 CRL，直到最后一张下级证书过期。
3. 生成和管理 CA 密钥对时，严格遵守密钥规范。
4. 及时发布新的 CA 证书。
5. 确保整个过渡过程安全、顺利，不出现信任真空期。

Prior to the expiration of certificate, GDCA will replace the root key in accordance with the provisions of CP, and generate a new certificate. When generating the new key, specifications of GDCA key management will be followed strictly. CA key changeover must comply with the following principles:

1. The new subordinate certificates can't be issued before the end of the life cycle of subordinate certificate, which ensures that all subordinate certificates are all expired as the CA certificates expired.
2. From the end of the issue of a new subordinate certificate to the expiration of the certificate, CA continues to sign CRLs with the original private key until the last subordinate certificate expires.
3. CA key generation and management must strictly follow the key regulations.
4. Release the new CA certificate timely.
5. Ensure the entire transition process safely, smoothly and no vacuum of trust.

GDCA 的管理员证书密钥更换由 KM 业务管理员提出申请。密钥更换时，GDCA 需要签发三个新证书：

- 新私钥签名的包含新公钥的 GDCA 证书；
- 新私钥签名的包含旧公钥的 GDCA 证书；
- 旧私钥签名的包含新公钥的 GDCA 证书。

The changeover of certificate key of GDCA administrator is applied by the KM services administrator. During the key replacement, CA should issue three new certificates:

- GDCA certificate with new public key signed by new private key;
- GDCA certificate with old public key signed by new private key;
- GDCA certificate with new public key signed by old private key.

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

为了及时响应和处理事故和损害发生的情况，GDCA 建立了一系列应急处理预案和事故处理方案，例如：

1. GDCA 系统故障处理规范
2. GDCA 重大事故应急预案
3. GDCA 系统备份与恢复方案

相关岗位的工作人员将按照以上方案和相关制度的规定，积极实施抢修恢复计划和措施，每季度进行数据灾难恢复演练，每年进行一次重大事故应急演练。

In order to timely respond to and handle accidents and damages, GDCA establishes a series of emergency response schemes and accident treatment schemes, for example:

1. GDCA system fault treatment specification.
2. GDCA major accident emergency scheme.
3. GDCA system backup and recovery scheme.

Related personnel will actively carry out the recovery plans in accordance with the regulations of the above schemes and related systems. And perform the data disaster recovery drill each quarter, and an emergency response drill on major accidents annually.

GDCA 制定并维护了全面且可执行的大规模撤销事件响应计划，该计划适用于其签发的所有 SSL/TLS 证书。GDCA 每年都会对该大规模撤销计划进行测试，以持续提升其应对大规模撤销事件的准备能力。

GDCA 的大规模撤销计划包含明确、可执行且全面的操作流程，旨在确保在大规模证书撤销情境下能够快速、一致且可靠地响应。GDCA 会将该计划提供给第三方审计人员进行审计，并每年对该计划进行测试、审查和更新。

该大规模撤销计划的内容符合 Baseline Requirements 第 5.7.1.2 节的相关规定。

GDCA has developed and maintained a comprehensive and actionable plan for mass revocation events, which is applicable to all SSL/TLS certificates it issues. GDCA performs annual testing of the mass revocation plan to continually improve its preparedness for mass revocation events over time.

GDCA's mass revocation plan includes clearly defined, actionable, and comprehensive procedures designed to ensure rapid, consistent, and reliable response to large-scale certificate revocation scenarios. GDCA will make this mass revocation plan available to our third-party auditors for review upon request and will annually test, review, and update this plan.

The mass revocation plan includes the contents as required by section 5.7.1.2 of the Baseline Requirements.

5.7.2. 计算资源、软件和或/数据的损坏 Computing Resources, Software, and/or Data Are Corrupted

GDCA 对业务系统及其他重要系统的资源、软件及数据进行了备份，并制定了相应的应急处理流程。当发生网络通信资源毁坏、计算机设备不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，GDCA 将按照灾难恢复计划实施恢复。

GDCA backs up resources of the business system and other important system, software and data and formulates corresponding emergency treatment process. When identified the destruction of network communication resources, failures of devices for daily services, malfunction of software, or tampered database etc., GDCA will launch the disaster recovery plan.

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、遗失、被篡改或泄露，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。如果需要撤销 CA 证书，将会采取以下措施：

1. 立即向电子认证服务管理办公室和其他政府主管部门汇报，通过网站和其他公共媒体对订户进行通告，采取措施避免用户利益遭受更大损失。
2. 立即通知相关依赖方关闭与证书认证服务相关的系统。
3. 立即撤销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。同时 GDCA 立即生成新的密钥对。
4. 新的根证书签发后，按照 GDCA CPS 关于证书签发的规定，重新签发下级证书和下级操作中级 CA 证书。
5. GDCA 新的证书签发后，将立即通过 GDCA 信息库、目录服务器、HTTP 等方式发布。

When CA root private key has been damaged, missed, tampered or leaked, GDCA will launch 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. GDCA reports immediately to the electronic authentication service management office and other government departments through the website and other public media to notify subscribers, and takes measures to protect user's interests against any further losses.
2. GDCA notifies the relevant parties to disconnect the systems associated with the certificate

authentication services immediately.

3. GDCA revokes immediately all the certificates issued, and updates CRL and OCSP information for subscribers and relying parties. Meanwhile GDCA immediately generates a new key pair.

4. After the new root certificate has been issued, GDCA Re-issues the certificates and the subordinate CA certificate in accordance with the GDCA CPS about provisions of certificates issuing.

5. After the new root certificate has been issued by GDCA, it will be immediately published by GDCA repository, LDAP, HTTP, etc.

当中级 CA 私钥出现遗失、被篡改、破解、泄露或被第三者窃用的疑虑时，操作 CA 应：

1. 立即向 GDCA 进行汇报并生成新的密钥对和证书请求，申请签发新的证书。
2. GDCA 立即向电子认证服务管理办公室和其他政府主管部门汇报，通过网站和其他公共媒体对订户进行通告，采取措施避免用户利益遭受更大损失。
3. 立即通知相关依赖方关闭与证书认证服务相关的系统。
4. 立即撤销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。
5. 新的中级 CA 证书签发后，按照 GDCA CPS 关于证书签发的规定，重新签发订户证书。
6. GDCA 新的证书签发后，将立即通过 GDCA 信息库、目录服务器、HTTP 等方式进行发布。

If private key of GDCA Subordinate CA is missing, tampered, cracked, leaked or used by unauthorized third parties suspiciously, Subordinate CA should:

1. Subordinate CA reports immediately to the GDCA and generates a new key pair and certificate request to apply for a new certificate.

2. GDCA reports immediately to the electronic authentication service management office and other government departments through the website and other public media to notify subscribers, and takes measures to protect user’s interests against any further losses.

3. GDCA notifies the relevant relying party to close the system associated with the certificate authentication services immediately.

4. All the certificates issued by the Subordinate CA are revoked immediately to update information on CRL and OCSP for querying of certificate subscriber and relying party.

5. Subscriber certificate is re-issued in accordance with the CPS about provision of a certificate issued after the new Subordinate CA certificate has been issued.

6. After the new root certificate has been issued, it will be immediately published by the GDCA

repository, LDAP, HTTP, etc. for distribution.

证书订户的私钥可能出现损毁、遗失、破解、被篡改，或者被第三者窃用时，订户应按照 GDCA CPS 的规定，首先申请证书撤销，并按照规定重新申请新的证书。

When private key for subscriber certificate is damaged, missing, cracked, tampered or used by unauthorized third parties suspiciously, the subscriber should apply for certificate revocation immediately and re-apply the new certificate following the provisions with the CPS of GDCA.

5.7.4. 灾难后的业务连续性能力 Business Continuity Capabilities After a Disaster

GDCA 在遭遇本节 5.7.1、5.7.2 和 5.7.3 中描述的灾难后，通过其备份机制，将在 24 小时之内恢复各项业务的正常运行。

After encountering the disaster described in section 5.7.1, 5.7.2 and 5.7.3, GDCA can use the backup mechanisms to recover systems for operation and service delivery within 24 hours.

5.8. 电子认证服务机构或注册机构的终止 CA or RA Termination

GDCA 终止事件的原因可以分为密钥受损原因和非密钥受损原因，密钥受损原因可能包括 GDCA 根密钥丢失，非密钥受损原因可能与商业因素有关。

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 停止相关的实体；
4. 关闭从目录服务器；
5. 证书撤销；
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。

The reason of GDCA termination event can be key damage or non-key damage. Key damage may be resulted from the loss of GDCA root key, and non-key damage reason may be related to commercial factors.

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.

由于密钥受损和非密钥受损原因而终止 GDCA，几乎要完成相同的操作，唯一的不同在 GDCA 终止发送通知的时间限制上，由于密钥受损原因终止 GDCA，要求 GDCA 通知订户的过程尽快完成；由于非密钥受损原因终止 GDCA，在 GDCA 通知所有订户后，采取适当的步骤减轻 GDCA 终止对订户的影响。

With the termination of GDCA due to key damage and non-key damage, the operations are mostly the same. The only difference is time limitation of GDCA stopping sending notification. As for GDCA termination due to key damage, the process in which GDCA notifies the subscriber needs to be completed as soon as possible. As for GDCA termination due to non-key damage, it can take appropriate measures to mitigate the effects of GDCA termination on the subscriber after GDCA notifies all the subscribers.

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 CA Key Pair Generation

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 CPS 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. Since FIPS140-2 is not a standard approved and accepted by OSCCA and OSCCA implements a strict management of state's cryptographic products, GDCA only applies part of the provisions of FIPS140-2 under the permission of OSCCA. Specifically, the product manual of the device is for your reference. Hardware Security Module used for key generation must be evaluated 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 CPS 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 for SubscriberKey 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 should 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

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 are 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

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. 电子认证服务机构公钥传送给依赖方 CA Public Key Delivery to Relying Parties

GDCA 的公钥包含在 GDCA 自签发的根 CA 证书和业务 CA 证书中，通过 GDCA 官方网站进行发布。GDCA 支持从 GDCA 的网站下载的方式传递公钥，以供证书订户和依赖方查询使用。

Public keys of GDCA are included in the self-signed root CA certificate and business CA certificate of GDCA and published through GDCA's official website. Subscribers and relying parties can download public keys from this website.

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管理局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。

对于参数质量的检查，同样由通过国家密码管理局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。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.

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 的根 CA 密钥仅用于签署以下证书：

1. 代表根 CA 的自签证书；
2. 中级 CA 的证书及交叉证书；
3. 用于基础设施的证书（如 OCSP 响应验证证书）。

Root CA keys of GDCA are used to sign the following certificates only:

1. Self-signed certificates to represent the root CA itself;

2. Certificates for subordinate CAs and cross certificates;

3. Certificates for infrastructure purposes (e.g. OCSP Response verification Certificates).

订户的密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等；加密密钥对可以用于信息加密和解密。

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

Subscriber's key can be used for providing security services, such as identity authentication, non-repudiation and the integrity of information, etc. Encryption key pair can be used to encrypt and decrypt information.

Authentication of identity, authorization of management, confirmation of responsibility and other security mechanisms can be done via using signing key and encryption key.

6.2. 私钥保护和密码模块工程控制 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. 密码模块的标准和控制 Cryptographic Module Standards and Controls

GDCA 所用的密码模块都是经国家密码管理局认可的产品，符合《GM/T 0028-2014 密码模块安全技术要求》，该标准与 FIPS 140-2 标准等同。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。

Cryptographic modules used by GDCA are approved and licensed by OSCCA and comply with < GM/T 0028-2014 Security Requirements for Cryptographic Modules>, a standard equivalent to FIPS 140-2. 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

GDCA 私钥的生成、更新、撤销、备份和恢复等操作采用多人控制机制，即采取五选三方式，将私钥的管理权限分散到 5 位密钥管理员中，至少在其中三人在场并许可的情况下，插入管理员卡并输入 PIN 码，才能对私钥进行操作。

Generation, update, revocation, backup and recovery operations, etc. of GDCA private key adopt multi-person control mechanisms. Namely, the mechanism is three out of five, means the key management authority is distributed to five key administrators, the operation of private key is performed in the presence and permission of no less than three employees via inserting cards of

administrators and inputting their PIN code.

6.2.3. 私钥恢复 Private Key Recovery

GDCA 密钥管理中心的密钥采用密钥恢复机制，对密钥管理中心生成的加密密钥对由 GDCA 管理，确保对任何使用密钥加密的数据都能依照法律流程进行司法恢复。

The GDCA key management center adopts a key recovery mechanism, with the encryption key pairs generated by the key management center being managed by the GDCA, ensuring that any data encrypted with these keys can be legally recovered in accordance with judicial procedures.

6.2.4. 私钥托管 Private Key Escrow

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，订户加密证书对应的私钥由 GDCA 托管，订户的签名证书对应的私钥由自己保管，GDCA 不负责托管。

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 不对订户私钥进行托管。

For the subscriber certificates issued by the subordinate CAs of ROOTCA (RSA), GDCA ROOT CA, ROOTCA (SM2), and GDCA ROOT CA1, the private key of encryption certificate is escrowed by GDCA. The private key of signing certificate is managed by subscriber and not escrowed by GDCA.

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 does not escrow the private keys of the subscribers.

6.2.5. 私钥备份 Private Key Backup

CA 私钥备份分为两种类型的备份：初始化备份（当第一次安装系统后就需进行备份）、完全备份（定期对系统中私钥库制作拷贝）。

初始化备份是系统初始化生成时进行的私钥备份。

完全备份是指私钥库的备份采用专门的备份软件进行完整备份，每周一次。

Private keys backup for CAs includes two types: initial backup (backup in the first installation), complete backup (regular copies of private key library in the system).

Initial backup is private key backup in the system installation.

Complete backup is complete backup of private key library once a week.

6.2.6. 私钥归档 Private Key Archival

GDCA 密钥管理中心对所生成的密钥信息进行归档保存，保存的方式为将密钥加密并保存在密钥管理中心的数据库中。

私钥到期后，GDCA 在 10 天内完成归档操作。私钥归档保存至少 7 年。

The GDCA key management center archives and preserves the generated keys by encrypting the keys and storing them in the database of the key management center.

Once private key expires, GDCA will complete archiving operation in 10 days. The validity of archiving private key is at least 7 years.

6.2.7. 私钥导出、导入密码模块 Private Key Transfer Into or From a Cryptographic Module

所有的密钥都必须在密码模块中产生，密码模块中的私钥不能以明文的形式导出。

对 CA 系统，在需要备份或迁移 CA 密钥时，从密码模块中导出的密钥必须加密，用于加密 CA 密钥的私钥由多人控制。备份的密钥恢复到密码模块中也由多人控制。

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。

All keys must be generated in cryptographic modules, and private keys in the cryptographic modules cannot be exported in plaintext.

For the CA system, when it is necessary to transport or backup the CA keys, the keys exported from the cryptographic module must be encrypted, and the private keys used to encrypt the CA key must be under multiple person control. Importation of the keys into the cryptographic modules must also under multiple person control.

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.

6.2.8. 私钥在密码模块的存储 Private Key Storage on Cryptographic Module

CA 系统的密码设备采用国家密码管理局批准和许可的服务器密码机，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，私钥的数据存储在服务器密码机硬

件中，在整个生命周期都不会明文出现在硬件密码机之外。

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。

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 equipment used by CA systems had been approved and permitted by OSCCA, and hardware cryptographic module at least meets the FIPS 140-2 level 3 standards or equivalent security levels. Private keys will not be in the form of text outside the hardware cryptographic modules in the entire life cycle.

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.

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.

6.2.9. 激活私钥的方法 Methods of Activating Private Key

密钥管理员使用自己的管理员卡登录服务器密码机，进行激活私钥的操作，需要三名管理员同时在场。

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。

Key administrators use their own administrative cards to login cryptographic server. Three administrators need to be at presence for private key activating operation.

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.

6.2.10. 解除私钥激活状态的方法 Method of Deactivating Private Key

密钥管理员使用含有自己的管理员卡登录服务器密码机，进行解除私钥的操作，需要三名管理员同时在场。

一旦私钥被激活，除非这种状态被解除，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。

GDCA 解除私钥激活状态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。未经授权的任何人员，绝不可以进行相关操作。

订户解除私钥激活状态由其自行决定，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，私钥就被解除。

Key administrators use their own administrator card to login cryptographic server and deactivate the private key. Three administrators at presence can execute above operation.

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.

The ways of deactivating private key include exit, shutdown, removing hardware cryptographic module and logout of user or system. Unauthorized person cannot execute above operation.

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.

6.2.11. 销毁私钥的方法 Method of Destroying Private Key

如果私钥不再被使用，或者与私钥相对应的公钥到期或者被撤销后，如果其处于软件加密模块内，那么该软件加密模块必须被覆盖方式清除；如果位于硬件加密模块内，那么加密设备或者 IC 卡等必须被清空为零。同时，所有用于激活私钥的 PIN 码、IC 卡等也必须被销毁或者收回。

订户的私钥不再被使用，或者与私钥相对应的公钥到期或者被撤销后，由订户决定其销毁方法，订户必须保证有效销毁其私钥，并承担有关的责任。涉及到密钥到期后保存和归档的，订户必须按照本 CPS 的规定执行。

If the private key is no longer in use, or after the corresponding public key is expired or revoked, for

the circumstance that the key is in software encryption module, it must be cleared by methods of mulching. For the circumstance that the key is in hardware encryption module, it should be cleared in the encryption device or IC card. Meanwhile, all the PIN codes, IC cards for activating private key also must be destroyed or recovered.

Private key no longer being used, or the public key corresponding to private key expired or revoked, the method of destruction is determined by the subscriber. The subscriber must destroy the private key effectively and assume the relevant responsibilities. Storage and archive of the key after expiration must conform to the provisions of this CPS.

6.2.12. 密码模块的评估 Cryptographic Module Rating

GDCA 使用国家密码管理局批准和许可的密码产品。

GDCA uses the cryptographic products approved and permitted by OSCCA.

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

对系统产生的公钥数据进行定时的归档保存，对保存的公钥信息进行对称加密，确保能获取安全完整的公钥信息。

公钥到期后，GDCA 在 10 天内完成归档操作。

GDCA should carry out archiving and preservation timely for public key data generated by the system and use symmetric encryption for public key information. Ensure to obtain the safe and complete public key information.

If public key has expired, GDCA should complete archiving operation in 10 days.

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。

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。

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。

The usage period of public key and private key is related to the validity period of certificate, but they are not completely consistent.

For the signing certificate, its private key can only be used for signing within the certificate validity period and not be used beyond 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 beyond the validity period of certificate.

For the encryption certificate, its public key can only be used for encryption within the validity period of certificate and not be used beyond 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 beyond 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。

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。

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。

For the certificate used for authentication, the private key and public key can only be used within the validity period of certificate.

If a certificate has multiple usages, the usage periods of public key and private key follow the rules described above.

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 RSA2048 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 bits 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 bits 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 bits root CA certificate, the maximum usage period of the key pair is 30 years or less than 30 years.
7. For the RSA 2048 bits 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 bits 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

为了保护私钥的安全，证书订户生产和安装激活数据必须保证安全可靠，从而避免私钥被泄漏、被偷窃、被非法使用、被篡改、或者被非法授权的披露。

CA 私钥的激活数据，必须按照有关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。订户私钥的激活数据，包括用于下载证书的口令（以密码信封等形式提供）、USB Key、IC 卡的登陆口令等，都必须在安全可靠的环境下随机产生。

GDCA 产生的激活数据，包括用于下载证书的口令（（以密码信封等形式提供）、USB Key、IC 卡的登陆口令等，都是在安全可靠的环境下随机产生。这些激活数据，都是通过安全可靠的方式，例如离线当面递交、邮政专递等方式交给订户。对于非一次性使用的激活数据，GDCA 建议用户自行进行修改。

Subscriber must use secure and reliable generation and installation of activation data to protect the private key from exposure, theft, unauthorized usage, modification, or unauthorized disclosure.

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.

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.

Activation data generated by GDCA, 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. The activation data are delivered to subscribers safely and reliably, such as through offline face-to-face submission, post courier delivery, etc. For activation data of non-single usage, GDCA suggests users to modify by themselves.

所有的保护口令都应该是不容易被猜到的，应该遵循以下几个原则：

1. 至少 8 位字符
2. 至少包含一个小写字母
3. 不能包含很多相同的字符
4. 不能和操作员的名字相同
5. 不能使用生日、电话等数字
6. 用户名信息中的较长的子字符串

All the protection passwords should not be something easily guessed, and should follow the following principles:

1. Contain at least eight characters
2. Contain one lowercase letter at least
3. Not contain many of the same characters
4. Not be the same as operator’s name
5. Not use birthdays, telephone numbers
6. Longer substring in user name information

6.4.2. 激活数据的保护 Activation Data Protection

对于 CA 私钥的激活数据，必须将激活数据按照可靠的方式分割后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。

订户的激活数据必须在安全可靠的环境下产生，必须进行妥善保管，或者记住以后进行销毁，不可被他人所获悉。如果证书订户使用口令或 PIN 码保护私钥匙，订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书订户使用生物特征保护私钥，订户也应注意防止其生物特征被人非法窃取。同时为了配合业务系统的安全需要，应该经常对激活数据进行修改。

Activation data of CA private key must be separated in a reliable way and kept by different trusted

personnel. Administrator must meet the requirements of responsibility division.

Subscriber's activation data must be generated in the safe and reliable environment and be properly safeguarded or destroyed, and cannot be leaked to others. If the certificate subscriber uses a password or PIN to protect private key, the subscriber should take good care of password or PIN to prevent the leakage or theft. If the certificate subscriber uses biological characteristics to protect the private key, the subscriber should also pay attention to prevent his/her biological characteristics from illegal obtaining. 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，应保护他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。

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者全部，比如记录有口令的在纸页必须粉碎。

考虑到安全因素，对于申请证书的订户激活数据的生命周期，规定如下：

1、订户用于申请证书的口令，申请成功后失效。

2、用于保护私钥或者 IC 卡、USB Key 的口令，建议订户根据业务应用的需要随时予以变更，使用期限超过 3 个月后应要进行修改。

Activation of private key shall be protected from loss, theft, modification, unauthorized disclosure, or unauthorized usage during the transmission.

The activation data of private key which is no longer used should 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.

For the security reasons, the rules of certificate applicant activate data of lifecycle as below:

1. The password used to apply for certificate becomes invalid after successful application.
2. The password used to protect the private key, or IC card, USB Key, could be modified by subscriber at any time based on business application, and should be modified three months after the validity.

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，按照国标《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 " Information security technology—Specifications of cryptograph and related security technology for certificate authentication system" published by OSCCA, "Measures for the Administration of Electronic Certification Services" published by Ministry of Industry and Information Technology, standards of information security in ISO 27001 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.

实行严格的双因素验证机制，为每位拥有系统（包括 CA 系统、RA 系统）访问权限的人员分配唯一的账户，账户的访问权限限制为执行工作职责要求的最小权限。访问时同时采用用户名、口令以及数字证书双因素登录方式。

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。

Dual-factor authentication mechanism shall be utilized in the login process to validate the digital certificate and username/password of user. GDCA assign each user of CA/RA system a unique account with minimum permissions according to the requirements of user.

Strict security controls ensures that the system of CA software and data files is secure and reliable and will not be accessed without authorization.

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 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 的认证系统、计算机及网络安全，每年由国家密码管理局主管部门对认证系统、计算机、网络安全进行年度评估审查，如有必要，根据相关专家及领导意见，对认证系统及系统安全进行升级改造。

GDCA certification systems pass the security review of OSCCA.

Authentication system, computer and network security of GDCA should be evaluated by OSCCA each year. According to the opinion of the relevant experts and leaders, GDCA may upgrade the authentication system and system security when necessary.

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. 制定公司内部的升级变更申请制度，并要求工作人员严格按照流程执行；
2. 制定公司内部的采购流程及管理制度；
3. 开发程序必须在开发环境进行严格测试成功后，再申请部署于生产环境；
4. 变更部署前进行有效的在线备份；
5. 第三方验证和审查；
6. 安全风险分析和可靠性设计；

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. Establish internal system of corporation about update, alteration and application. The employees should follow this system strictly.
2. Establish internal purchasing process and management system of corporation.
3. After the programs have passed strict test in development environment, they can be deployed to production environment.

4. Effective online backup must be done before deployment changes.
5. Verification and review of third-party.
6. 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，严格遵循国家密码管理局的有关运行管理规范进行操作。

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 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。

Information security management of GDCA certification system conforms to the relevant operation management specification of OSCCA strictly.

GDCA authentication system has a strict control measures, and all the systems can be used only after being rigorously tested and verified. 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 on certification system.

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具备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。

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。

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.

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。

认证系统只开放与申请证书、查询证书等相关的操作功能，供用户通过网络进行。只有 GDCA 授权的员工能够进入 GDCA 证书服务器、GDCA 证书目录服务器、GDCA 操作中心等设备或系统。

为了确保网络安全，GDCA 认证业务系统安装部署了入侵检测、安全审计、防毒防范和网管系统，并且及时更新防火墙、入侵监测、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。

GDCA authentication system has multi-level firewalls and the protection of network resource security control systems. It also has complete access control technology.

Authentication system only provides the operations such as application and query of certificate to subscribers over the network. Only employees authorized by GDCA can access the GDCA certificate server, GDCA certificate directory server, GDCA operation center and other equipment or systems.

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 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 Certificate Profile

GDCA 使用的详细证书格式符合国家相关标准要求，是 ITU-T 推荐的一个国际标准 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）。

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。

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 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 CPS 第 7.1.3 节）
签发者	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本 CPS 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 CPS 7.1.3 中指定的算法，密钥长度满足 CPS 指定的要求。

Following are the basic certificate fields for the certificates issued by GDCA:

Fields	Value or value limit
Version	The format version of X.509 certificate with a value of V3.
Serial Number	The unique identifier of a certificate.

Signature Algorithm	The signature algorithm used to issue certificates (Section 7.1.3 of this CPS).
Issuer	Issuer's distinguished name, including CN, O, and C.
notBefore	Based on Coordinated Universal Time (UTC), synchronized with Beijing time, encoded according to RFC 5280.
notAfter	Based on Coordinated Universal Time (UTC), synchronized with Beijing time, encoded according to RFC 5280.
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, 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 (Optional), 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	Encoded according to RFC 5280, using the algorithms specified in section 7.1.3 of this CPS, with key sizes meeting requirements specified in this CPS.

7.1.1. 版本号 Version Number(s)

GDCA 证书符合 X.509 V3 版证书格式，版本信息存放在证书版本格式栏内。

GDCA certificates are compliant with X.509 V3 certificate format. The version information is listed in

the version field of the certificate.

7.1.2. 证书扩展项 Certificate Extensions

GDCA 除了使用 X.509 V3 版证书标准项和标准扩展项以外，还使用了自定义扩展项。

In addition to the X.509 V3certificate standard items and standard extension items, GDCA also uses customized 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 CPS 的第 1.4.1.8 节。

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 CPS.

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 CPS 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，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 CPS.

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 CPS 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. 统一社会信用代码号：用于表示企业的统一社会信用代码。
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 CPS.

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 CPS 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 CPS 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 CPS 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 CPS.

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

证书策略对象标识符同本 CPS 第 1.4.1.8 节。

See CPS section1.4.1.8.

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规则 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。

GDCA issues CRL regularly for the subscribers to query.

7.2.1. 版本 Version Number(s)

GDCA 的证书撤销列表采用 X.509 v2 格式。

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

7.2.2. CRL 和 CRL 条目扩展项 CRL and CRL Entry Extensions

GDCA 的证书撤销列表（CRL）是一个带有时间戳并且经过数字签名的已撤销证书

的列表。CRL 的签发者是 CA，GDCA 通过发布 CRL 提供它所签发的数字证书的状态信息。

1. CRL 的版本号：用来指定 CRL 的版本信息，GDCA 采用的是同 X.509 V3 证书对应的 CRL V2 版本。
2. 签名算法：GDCA 采用 sha1 RSA、sha256RSA、sha256ECDSA、SM2 及 ECC 签名算法。
3. 颁发者：指定签发机构的 DN 名，由国家、省、市、机构、单位部门和通用名等组成。
4. 生效时间：指定一个日期/时间值，用以表明本 CRL 发布的时间。
5. 更新时间：指定一个日期/时间值，用以表明下一次 CRL 将要发布的时间（本标准强制使用该域）。
6. 撤销证书列表：指定已经撤销的证书列表。本列表中含有证书的序列号和证书被撤销的日期和时间。
7. 颁发机构密钥标识符（Issuer Unique Identifier）：本项标识用来验证在 CRL 上签名的公开密钥。它能辨别同一 CA 使用的不同密钥。
8. 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 CPS 第 4.9.1 中最相关的理由。

CRL is a revoked certificate list with time stamp and digital signature. The issuer of CRL is CA. GDCA provides certificate status information through releasing CRL.

1. CRL version: It refers to version information of CRL, GDCA adopts CRL V2 corresponding to X.509 V3 certificate.
2. Signature algorithm: GDCA adopts sha1 RSA, sha256RSA, sha256ECDSA, SM2 and ECC signature algorithms.
3. Issuer: It refers to DN of issuing authority, including country, province, city, organization, department and common name, etc.

4. Effective time: It refers to date/time which indicates CRL issuing time.

5. Update time: It refers to date/time which indicates next issuing time of CRL. (It's an enforced field in this CPS).

6. Certificate Revocation List: It refers to a list of revokedcertificates. The list contains certificate serial number and certificate revocation date and time.

7. Issuer Unique Identifier: It is used to authenticate the public key which is used to verify signature of CRL. It can distinguish different keys used by the same CA.

8. 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 CPS.

7.3. 在线证书状态协议 OCSP Profile

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。在 GDCA 官方网站下载 OCSP 查询客户端并按照 GDCA 官方网站发布的 OCSP 操作说明进行配置，即可使用 GDCA 的在线证书状态查询服务。GDCA 签发的 OCSP 响应至少包含以下所述的 OCSP 机构基本域和内容：

1. Version：客户端使用的 OCSP 协议的版本号；GDCA 的在线证书状态协议为 v1 版。
2. signatureAlgorithm：签发 OCSP 的算法。
3. responderID：签发 OCSP 的实体。签发者公钥的 SHA1 数据摘要值和证书甄别名。
4. producedAt：OCSP 响应生成的日期和时间。
5. Signature：OCSP 响应消息的数字签名。
6. Nonce(一次性随机数)：在状态请求消息中的每一个 requestExtensions 变量和响应消息中的 responseExtension 变量中包含一次性随机数，防止重放攻击。
7. 证书状态：证书的最新状态，包括有效、撤销和未知。

   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 CPS 第 7.2.2 章中允许的理由码。

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. Subscribers can download the OCSP query client from GDCA official website and follow the OCSP guide book published at GDCA official website for configuration. Then subscribers can use GDCA's online certificate status query service. OCSP response message issued by GDCA contains at least OCSP organization basic domains and contents described below:

1. Version: OCSP protocol version number used by client. The version of GDCAOCSP is v1.
2. SignatureAlgorithm: Algorithm used for signing and issuing OCSP.
3. ResponderID: ID of entity who issues OCSP. It consists of SHA1 of issuer’s public key and DN of certificate.
4. ProducedAt: Date and time when OCSP response message is generated.
5. Signature: Digital signature of OCSP response message
6. Nonce: The nonce, which is used to prevent replay attacks, is included in requestExtensions variable of state request message and responseExtension of response message.
7. Certificate status: The latest status of a certificate, the status can be valid, revoked, and unknown.

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 CPS.

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 请求和响应处理 OCSP Request and Response Resolution

一个 OCSP 请求包含以下数据：协议版本、服务要求、目标证书标识和可选的扩展项等。在接受一个请求之后，OCSP 服务端响应时进行如下检测：

- 信息正确格式化
- 响应服务器被配置提供请求服务
- 请求包含了响应服务器需要的信息，如果任何一个先决条件没有满足，那么 OCSP

服务端将产生一个错误信息；否则的话，返回一个确定的回复

Protocol version, service request, target certificate identifier and optional extensions, etc.

After receiving a request, OCSP server does the following tests during response:

- Information is formatted correctly
- The response server is configured to provide the request services
- The request contains all the information needed by response server. If any pre-condition is not met, the OCSP server will return an error message. Otherwise, it returns a determinate response.

所有确定的回复都由 GDCA 证书签发者密钥进行数字签名，主要回复状态包括：证书有效、已撤销、未知。回复信息由以下部分组成：

- 回复语法的版本
- 响应服务器名称
- 对请求端证书的回复
- 可选扩展
- 签名算法对象标识符号
- 对回复信息散列后的签名

All determinate responses are signed by GDCA certificate issuer. The main response statuses are valid, revoked, and unknown. The response message consists of the following components:

- Reply syntax version
- Response server name
- Response to the request client certificate
- Optional extensions
- Signature Algorithm object identifier
- The signature after the response information is hashed

如果出错，OCSP 服务器会返回一个出错信息，这些错误信息没有 GDCA 证书签发者密钥的签名。出错信息主要包括：

- 未正确格式化的请求（malformedRequest）
- 内部错误（internalError）
- 请稍后再试（trylater）
- 需要签名（sigRequired）
- 未授权（unauthorized)

If an error occurs, OCSP server will return an error message, which doesn't contain key signature

signed of GDCA certificate issuer. The error message includes:

- malformedRequest
- internalError
- trylater
- sigRequired
- unauthorized

7.3.3. 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. 评估的频率或情形 Frequency or Circumstances of Assessment

GDCA 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 conducts an internal 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 CAs 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 CPS 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，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 CA 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 CPS. 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/资质 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 are no business interactions, 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. 评估内容 Topics Covered by Assessments

GDCA 中心的审计工作包括以下内容：

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 CPS、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。

GDCA's audit contents include:

1) Whether the security strategy is fully implemented
2) Whether operation procedures and processes strictly followed
3) Whether strictly following the CPS, 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措施 Actions Taken as a Result of Deficiency

对于本机构审计结果中的问题，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，各职能部门需向审计评估小组提交业务改进工作总结报告。

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 CPS 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。

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。

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.

For authorized RA mentioned in GDCA's audit report, if they are violating the CPS 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.

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 的审计结果向本机构各职能部门以及审计涉及的证书注册机构进行正式通报，对可能造成订户安全隐患，GDCA 将及时向订户通报。

第三方审计师事务所评估完成后，对于审计的结果，将通过 https://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。

Audit results are formally informed to relevant departments of GDCA and related RA. GDCA will notify the subscribers of any potential security risks timely.

If the assessment from a third-party auditor firm is completed, the audit results will be published at GDCA website (https://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 8.1 章节。

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

9.1.1. 证书签发和更新 Certificate Issuance and Renewal 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 有权根据市场状况，针对不同订户群体推出不同的收费策略或优惠措施。

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。

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. GDCA has the rights to launch different charging and discount policies targeted to different subscriber groups.

If the price specified in GDCA agreements with subscribers is different from the one published, the agreement price prevails.

9.1.2. 证书查询费用 Certificate Access Fees

在证书有效期内，对该证书信息进行查询，目前 GDCA 不收取查询费用。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。

如果证书查询的收费政策有任何变化，GDCA 将会及时在网站 https://www.gdca.com.cn 上予以公布。

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.

If certificate inquiry charging policy has any changes, GDCA will promptly post the changes at its website (https://www.gdca.com.cn).

9.1.3. 证书撤销或状态信息的查询费用 Revocation or Status Information Access Fees

GDCA 对于证书撤销和状态查询，目前不收取任何费用。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。

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 https://www.gdca.com.cn 上予以公布。

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.

If revocation and status information inquiry charging policy has any changes, GDCA will promptly post the changes at its website (https://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 CPS 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 CPS 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。

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 CPS 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。

此退款策略不限制订户得到其它的赔偿。

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。

GDCA does not refund any fees to subscribers except fees charged for certificate application and renewal because of specific reasons.

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 CPS 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.

This refund policy does not limit users from obtaining other compensation.

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

出现下列情形并经 GDCA 确认后，证书订户、依赖方等实体可以申请 GDCA 承担赔偿责任（法定或约定免责除外）。

- GDCA 将证书错误地签发给订户以外的第三方，导致订户或者依赖方遭受损失的；
- 订户提供了虚假的注册信息或者资料，GDCA 发现后仍然签发了证书，导致依赖方遭受损失的；
- GDCA 未按鉴证要求对订户证书申请信息进行审核而签发了数字证书，导致订户或依赖方遭受损失的；
- 由于 GDCA 的原因导致证书私钥被破译、窃取，致使订户或者依赖方遭受损失的；GDCA 未能及时撤销证书的；
- GDCA 对于任何证书订户、依赖方等实体有关证书赔偿的合计责任限制在不超出证书购买价格的 10 倍。

对于 EV SSL 证书和 EV 代码签名证书，其赔偿金额遵循最新发布的《GDCA EV 证书电子认证业务规则》。对于特定应用场景下的证书业务，GDCA 也可以根据具体情况另行约定证书赔偿金额上限。

If the following circumstances occur and is confirmed by GDCA, certificate subscribers, relying

parties and other entities can request GDCA assume compensation liabilities (except for statutory or contractual exemptions). For the certification services for a particular application scenario, GDCA may stipulate other maximum compensation amount.

- GDCA issues certificates to a third-party instead of the subscriber by mistake, which leads to losses of the subscriber or relying party.
- After GDCA knows the fact that subscriber provides fake registration information or data, GDCA still issues certificate, which leads to relying party suffering losses.
- GDCA issues certificates without authenticating subscribers' application and it leads to the losses of subscribers or relying party.
- If the private key of the certificate is deciphered or stolen due to the fault of GDCA, which leads to the subscriber or relying party suffering losses. GDCA fails to revoke the certificate in time.
- The compensation maximum amount shall not exceed 10 times the purchase price of the certificate.

Compensation liabilities concerning EV SSL certificates and EV code signing certificates are stipulated in the latest version of the "GDCA EV CPS".

9.2.2. 其他资产 Other Assets

不适用。

Not Applicable.

9.2.3. 对最终实体的保险或担保 Insurance or Warranty Coverage for End-Entities

GDCA 如违反了本 CPS 中规定的职责，证书订户、依赖方等实体可以申请 GDCA 承担赔偿责任（法定或约定免责除外）。在经 GDCA 确认后，可以对该实体进行赔偿。赔偿限制如下：

1) GDCA 所有的赔偿义务不得超出本节 9.2.1 中规定的保险范围，赔偿金额不得高于赔偿金额上限，赔偿金额上限可以由 GDCA 根据情况重新制定，GDCA 会将重新制定后的情况立刻通知相关当事人。
2) GDCA 只有在证书有效期限内承担损失赔偿责任。

If GDCA violates the provisions of this CPS, certificate subscribers, relying party and other entities can request that GDCA shall assume the liability for compensation (except for statutory or contractual exemption). After confirmation, GDCA can compensate for the entity. Limitations of compensation are as follows:

1. All the compensation obligation of GDCA shall not exceed the insurance coverage stipulated in

section 9.2.1.The amount of compensation shall not be higher than the compensation maximum amount. GDCA can reset the compensation maximum amount. GDCA will notify relevant parties immediately after the reset.

2. GDCA only assumes compensation liabilities when the certificate is valid.

9.2.4. 责任免除 Liability Exemption

有下列情形之一的，应当免除 GDCA 之责任：

1. 订户在申请和使用 GDCA 数字证书时，有违反如下义务之一的：
   1) 订户有义务提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信息；
   2) 订户应当妥善保管 GDCA 所签发的数字证书载体和保护 PIN 码，不得泄漏 PIN 码或将数字证书载体随意交付他人；
   3) 订户在应用自己的密钥或使用数字证书时，应当使用可依赖、安全的系统；
   4) 订户知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知 GDCA 及相关各方，并终止使用该电子签名制作数据；
   5) 订户在使用数字证书时必须遵守国家的法律、法规和行政规章制度。不得将数字证书作为 GDCA 规定使用范围外的其他任何用途使用；
   6) 订户必须在证书有效安全期内使用该证书；不得使用已失密或可能失密、已过有效期、被冻结、被撤销的数字证书；
   7) 订户有义务根据规定按时向 GDCA 及当地业务受理点交纳服务费用。

If one of the circumstances below has occurred, the responsibilities of GDCA shall be exempted:

1. If one of the following obligations are violated when subscribers are applying and using GDCA digital certificates:
   1) The subscriber has the obligation to provide real, complete, accurate material and information, and forbid to provide fake, invalid materials and information;
   2) The subscriber shall properly keep the certificate carrier issued by GDCA and protect PIN code, and forbid to leak the PIN code or deliver the certificate carrier to others at discretion;
   3) When the subscribers are using their own keys or certificates, they shall use reliable and secure systems;
   4) If the subscriber has known data used for making electronic signature (private key) has been compromised or may have been compromised, he/she should inform GDCA and related parties promptly, and terminate the use of data used for making electronic signature;

5) Subscribers shall abide by national laws, regulations and administrative rules and regulations during the use of certificate. Subscribers are prohibited to use the certificates out of the scope which specified by GDCA;

6) Subscribers must use the certificate within the period of validity. Subscribers are prohibited to use certificates that have compromised or may have been compromised, expired, frozen or revoked;

7) Subscribers have obligations to pay the service fees to GDCA and local service acceptance points promptly.

2. 由于不可抗力原因而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“不可抗力”，是指不能预见、不能避免并不能克服的客观情况，包括但不限于：

1) 自然现象或者自然灾害，包括地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；

2) 社会现象、社会异常事件或者政府行为，包括政府颁发新的政策、法律和行政法规，或战争、罢工、骚乱等社会异常事件。

2. If the certificate has problems of issuance in error, delay, interruption, failure issuance, suspension, or termination in all or parts of the certificate services due to force majeure. "Force Majeure" refers to unforeseeable, unavoidable and insurmountable circumstances, including but not limited to:

1) Natural phenomenon or natural disaster: earthquake, volcano eruption, landslide, debris flow, avalanche, flood, tsunami, typhoon and other natural phenomenon.

2) Social phenomenon, social abnormal events or government actions: the government issues new policy, laws and administrative regulations, or other social abnormal events like war, strikes, chaos, and etc.

3. 因 GDCA 的设备或网络故障等技术故障而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“技术故障”引起原因包括但不限于：

1) 不可抗力；

2) 关联单位如电力、电信、通讯部门而致；

3) 黑客攻击；

4) GDCA 的设备或网络故障。

3. If the certificate has problems of issuance in error, delay, interruption, failure issuance, suspension, or termination in all or parts of the certificate services due to equipment, network or other technical failures of GDCA. "Technical Failure" refers to the following circumstances, including but not limited to:

1) Force majeure

2) Failure due to relevant departments such as electricity, telecommunication and communication departments

3) Hacker attacks

4) Equipment or network failure of GDCA

4. GDCA 已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

4. If GDCA has been compliant with certificate authentication rules defined by national laws and regulations, but the losses still occur.

在粤港互认项目，有以下情形的应当免粤港两地政府和电子认证服务主管部门的责任：

在遵守相关法律监管要求和《粤港电子签名证书互认证书策略》的基础上，应用在粤港互认和电子认证服务主管部门的证书以及相关行为，任何由于 GDCA 或相关证书的不足或疏忽所引起的责任和索偿，GDCA、订户和依赖方对粤港两地政府免责。

For the certificate of Hong Kong-Guangdong mutual recognition, the responsibilities of Guangdong, Hong Kong governments and electronic authentication services departments will exempt their responsibilities if the following circumstances have occurred:

On the basis of compliance with the relevant laws and regulatory requirements and the " Hong Kong-Guangdong mutual recognition of electronic signature certificates certificate policy", applying in the certificate of Guangdong Hong Kong mutual recognition and electronic certification service departments and related behavior, any responsibilities and compensations caused by shortage and negligence of the GDCA or related certificate, GDCA, subscribers and relying party can't claim the responsibilities from Guangdong and Hong Kong government.

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

GDCA 将以下信息视为不保密信息：

- 由 GDCA 发行的证书和 CRL 中的信息。
- 由 GDCA 支持、CPS 识别的证书策略中的信息。
- GDCA 许可，只有 GDCA 订户方使用，在 GDCA 网站公开发布的信息。
- 其他：GDCA 信息的保密性取决于特殊的数据项和申请。

GDCA treats the following information as non-confidential information:

- Information in the certificate and CRL issued by GDCA
- Information in certificate policy supported by GDCA and recognized by CPS
- Information that is permitted by GDCA, only used by GDCA subscribers and published at the GDCA website
- Others: The confidentiality of GDCA information depends on particular data items and applications

9.3.3. 保护保密信息的责任 Responsibility to Protect Confidential Information

GDCA 有妥善保管与保护本节 9.3.1 中规定的保密信息的责任与义务。

GDCA has the responsibility and obligation to protect the confidential information described in section 9.3.1.

9.4. 个人隐私保密 Privacy of Personal Information

9.4.1. 隐私保密方案 Privacy Plan

GDCA 尊重证书订户个人资料的隐私权，保证完全遵照国家对个人资料隐私保护的相关规定及法律。同时，GDCA 将确保全体职员严格遵从安全和保密标准对个人隐私给予保密。有关个人隐私保护相关的政策可以在 GDCA 官网（https://www.gdca.com.cn/）进行查询。

GDCA respects the privacy of the certificate subscriber's personal data and guarantees to fully comply with the relevant national laws and regulations. In the meantime, GDCA requires all employees strictly comply with security and confidential standards for personal privacy. Policies in relation to the personal privacy protection can be found at the GDCA website (https://www.gdca.com.cn).

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，GDCA 定义以下信息为证书订户的隐私信息：

- 订户的有效证件号码如身份证号码、单位机构代码。
- 订户的联系电话。
- 订户的通信地址和住址。
- 订户的银行帐号。

Except for the information already included in the subscriber certificates and the certificate status i nformation, other basic information provided by the subscribers is deemed private. GDCA defines the following information as certificate subscriber's privacy information:

- Subscriber's valid documents number such as ID number, organization code
- Subscriber's telephone number
- Subscriber's mailing address and living address
- Subscriber's bank account number

9.4.3. 不被视为隐私的信息 Information Not Deemed Private

GDCA 定义包括但不限于以下信息不被视为证书订户的隐私信息：

The information of certificates subscribers not deemed as private by GDCA include but not limited to the following:

- 订户姓名、单位名称等。
- 订户性别、单位性质等。
- 订户通信地址的邮政编码。
- 订户的电子邮箱。
- Subscriber’s name, organization name
- Subscriber’s gender, organization nature
- Subscriber’s postal code of mailing address
- Subscriber’s email address

9.4.4. 保护隐私的责任 Responsibility to Protect Private Information

GDCA 有妥善保管与保护本节 9.4.2 中规定的证书申请者个人隐私的责任与义务。

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 将采取适当的步骤保护证书订户的个人隐私，并将采取可靠的安全手段保护已存储的个人隐私信息。除非根据法律或政府的强制性规定，在未得到证书订户的许可之前，GDCA 保证不会把证书订户的除写入数字证书的个人资料外的个人信息提供给无关的第三方（包括公司或个人）。

GDCA takes appropriate steps to protect the certificate subscriber's personal privacy, and takes reliable security measures to protect stored personal privacy information. GDCA guarantees not to provide the certificate subscriber’s personal information, except personal information written in the certificate, to unrelated third parties (including companies and individuals), without the permission of certificate subscriber, unless base on provisions of the law or government.

9.4.6. 依法律或行政程序的信息披露 Disclosure Pursuant to Judicial or Administrative Process

当行政机关需要 GDCA 提供相应的证书使用者的相关信息时，GDCA 需提供如下信息：

- 订户的基本信息。

- 订户用个人加密密钥加密的信息。
- 订户对 GDCA 网站的登录情况。
- GDCA 将按照法律要求向执法人员提供相关信息。

When administrative organization requires GDCA to provide subscriber's information of corresponding certificates, GDCA needs to provide the following information:

- Subscriber's basic information
- Information encrypted by subscriber's personal encryption key
- GDCA website login information of subscribers
- GDCA will provide related information to law-enforcement officials in accordance with the law requirements.

9.4.7. 其他信息披露情形 Other Information Disclosure Circumstances

如果证书订户要求 GDCA 提供某类特定客户支援服务如资料邮寄时，GDCA 则需要把证书订户的姓名和邮寄地址等信息提供第三者如邮寄公司。

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

- 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。
- GDCA 对数字证书系统软件具有所有权、名称权、利益分享权。
- GDCA 有权决定采用何种软件系统。
- 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。
- GDCA 发行的证书和 CRL 均为受 GDCA 支配的财产。
- 对外运营管理策略和规范为 GDCA 财产。
- 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。
- GDCA reserves and remains full intellectual property rights for all the certificates and software offered by GDCA.
- GDCA holds ownership, the right of name, the right to share the benefits for certificate system software.

- GDCA has the right to decide to use which software system.
- All the information published at GDCA website is GDCA property. Without written permission of GDCA, others cannot repost them for commercial activities.
- Certificates and CRLs issued by GDCA are both the properties controlled by GDCA.
- External operation management strategy and specification are GDCA properties.
- 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. 电子认证服务机构的陈述与担保 CA Representations and Warranties

GDCA 在提供电子认证服务活动过程中的承诺如下：

- 签发给订户的证书符合 GDCA 的 CPS 的所有实质性要求。
- 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。
- 将根据 CPS 的要求及时撤销证书。
- 拒绝签发证书后，将立即向证书申请者归还所付的全部费用。
- 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；
- 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；
- 验证证书中所包含的全部信息的准确性（organizationalUnitName 信息除外）；
- 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；
- 根据 CPS 3.2 的要求验证申请人的身份；
- 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；
- 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。

During the process of providing electronic certification service activities, GDCA makes following commitments:

- Certificates issued to subscribers by GDCA must be in line with all substantive requirements of

this CPS.

- Informs subscribers any known events, which will fundamentally affect the validity and reliability of the certificate.
- Revokes the certificate according to this CPS.
- After refusing to issue a certificate, GDCA would immediately refund the fee that the applicant has paid for the certificate.
- 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).
- 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.
- Verifies the accuracy of all of the information contained in the certificate (with the exception of the organizationalUnitName information).
- Implements a procedure for reducing the likelihood that the information contained in the certificate's subject: organizationalUnitName attribute would be misleading.
- Verifies the identity of the applicant according to section 3.2 of this CPS.
- 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.
- Maintains a 24 x 7 publicly-accessible repository with current information regarding the status (valid or revoked) of all unexpired certificates.

证书公开发布后，GDCA 确保证书中的信息是经过验证的。

After the certificates have been issued and published, GDCA guarantees that the information contained in the certificate has been properly validated.

9.6.2. 注册机构的陈述与担保 RA Representations and Warranties

GDCA 的注册机构在参与电子认证服务过程中的承诺如下：

1. 提供给证书订户的注册过程完全符合 GDCA 的 CPS 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 CPS 的规定，及时向 GDCA 提交撤销、更新等服务申请。

During participation in the process of electronic certification services, registration authority of GDCA makes following commitments:

1. The registration process provided for subscribers is compliant with all the substantive requirements of GDCA CPS.
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 CPS.

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、注册机构及信赖证书的有关当事人作出以下承诺：

- 已知悉和接受 GDCA 的“数字证书申请责任书”和本 CPS 中的所有条款和条件。
- 在证书的有效期内进行数字签名。
- 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。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。
- 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。
- 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。
- 一经接受证书，即表示订户知悉和接受本 CPS 中的所有条款和条件，并知悉和接受相应的订户协议。
- 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。
- 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。
- 证书在本 CPS 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。
- 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。
- 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。

- 对于代码签名证书的订户，若发现以下情况，应立即向 GDCA 申请撤销证书：1）证书中的信息为或将成为错误或不准确的信息；2）证书中与公钥有关的私钥被误用或被损坏；3）有证据表明，该代码签名证书被用于签署可疑代码。

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:

- Acknowledged and accepted all the terms and conditions of GDCA "certificate application responsibility" and CPS.
- The subscriber uses digital signatures if the certificate is valid.
- 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.
- 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.
- Each signature is generated using the private key corresponding to the public key included in certificate by subscribers themselves. The certificates shall be valid at the moment of signing, i.e. certificate is not revoked or expired. The private key for the certificate is accessed and used by the subscriber itself.
- 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.
- Once the certificate is accepted, subscribers are considered as knowing and accepting all the terms and conditions in the CPS as well as corresponding subscriber agreements.
- Once the certificate is accepted, the subscriber should assume the following responsibilities: always maintain control of their private keys; use trustworthy systems; and take reasonable precautions to prevent the loss, disclosure, alteration, or unauthorized usage of the private keys.
- 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.
- The subscriber only uses certificate for the authorized or other lawful purpose within the range specified by this CPS.
- The subscriber use secure and reasonable measures to prevent the private key from loss, disclosure, alteration and other events.
- 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.

- Subscribers of code signing certificates shall promptly request the revocation of their certificates by GDCA in case of the following situations: 1) any information in the certificate is or becomes incorrect or inaccurate; 2) there is any misuse or compromise of the subscriber's private key associated with the public key included in the certificate; 3) there is evidence that such code signing certificates are used to sign suspicious codes.

9.6.4. 依赖方的陈述与担保 Representations and Warranties of Relying Party

- 遵守本 CPS 的所有规定。
- 确认证书在规定的范围和期限使用证书。
- 在信赖证书前，对证书的信任链进行验证。
- 在信赖证书前，通过查询 CRL 或 OCSP 确认证书是否被撤销。
- 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。
- 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。
- Abide by all provisions of this CPS.
- Ensure that the certificate is used in prescribed scope and duration.
- Verify certificate's trust chain before trust the certificate.
- Before trust a certificate, verify whether the certificate is revoked or not through querying CRL or OCSP.
- 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.
- 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

GDCA 从事电子认证活动的其他参与者作出如下承诺：

遵守本 CPS 的所有规定。

Other participants engaged in GDCA electronic certification activities make the following

commitments:

Abide by all provisions of this CPS.

9.7. 担保免责 Disclaimers of Warranties

除本 CPS9.6.1 中的明确承诺外，GDCA 不承担其他任何形式的保证和义务：

- 不保证证书订户、信赖方、其他参与者的陈述内容。
- 不对电子认证活动中使用的任何软件做出保证。
- 不对证书在超出规定目的以外的应用承担任何责任。
- 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。
- 订户违反本 CPS9.6.3 之承诺时，或依赖方违反本 CPS9.6.4 之承诺时，得以免除 GDCA 之责任。

Except for the commitments declared in CPS Section 9.6.1, GDCA does not assume any other forms of guarantee and obligation:

- Do not guarantee the statements of certificate subscribers, relying party and other.
- Do not guarantee any software used in electronic certification activities.
- Do not assume any liability when certificate is used beyond the prescribed purposes.
- Do not assume any responsibility for service interruption and customer losses caused by force majeure, such as war, natural disasters, etc.
- When subscriber violates the commitments defined in CPS Section 9.6.3, or relying party violates the commitments defined in CPS 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 将承担不超过本 CPS9.9 规定的有限赔偿责任。

If the certificate subscriber and the relying party specialized in civil activities suffered losses due to electronic certification services provided by GDCA, GDCA will assume limited compensation liability no more than the amount stipulated in the CPS Section 9.9.

9.9. 赔偿 Indemnities

9.9.1. GDCA 的赔偿责任 Indemnification by GDCA

如 GDCA 违反了本 CPS9.6.1 中的陈述，证书订户、依赖方等实体可以申请 GDCA 承担赔偿责任（法定或约定免责除外）。如出现下述情形，GDCA 承担有限赔偿责任：

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 的原因导致证书私钥被破译、窃取、泄露，导致订户或依赖方遭受损失的；
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 CPS 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 the certificate is deciphered, stolen or disclosed due to GDCA, which leads to the subscriber or relying party suffering losses.
5. GDCA fails to revoke certificates in time, which leads to relying party suffering losses.

另外，GDCA 赔偿限制如下：

1. GDCA 所有的赔偿义务不得高于本 CPS 9.2.1，这种赔偿上限可以由 GDCA 根据情况重新制定。
2. 对于由订户或依赖方的原因造成的损失，GDCA 不承担责任，由订户或依赖方自行承担。
3. GDCA 只有在证书有效期限内承担损失赔偿责任。

In addition, GDCA's compensation limitations are as follow:

1. All the compensation obligation of GDCA shall not exceed the insurance coverage stipulated in section 9.2.1. The maximum amount of compensation can be reset by GDCA based on different situations.
2. For the losses caused by subscribers or relying party, GDCA does not assume responsibilities. Subscribers or relying themselves should assume their own responsibilities.
3. GDCA assumes the liability for damages only when the certificate is valid.

9.9.2. 订户的赔偿责任 Indemnification by Subscribers

如因下述情形而导致 GDCA 或依赖方遭受损失，订户应当承担赔偿责任：

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 CPS 及相关操作规范，或者将证书用于非本 CPS 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 CPS 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. 提供的资料或信息不真实、不完整或不准确；
6. 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；
7. 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；
8. 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；
9. 证书到期但仍在使用证书；
10. 订户的证书信息侵犯了第三方的知识产权；
11. 在规定的范围外使用证书，如从事违法犯罪活动。

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

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 CPS and related operation practices when using certificates as well as using the certificates activities outside of the CPS.
4. If the certificate is used for illegal transactions or causes disputes during the period from revocation requests submitted by the subscribers or other entities authorized by GDCA to this information of certificate revocation published by GDCA, if GDCA operates in accordance with the requirements of the CPS, subscribers must assume any responsibility of losses according to this CPS.
5. Unreal, incomplete or inaccurate information provided by subscribers.
6. Subscribers continue to use the certificates and do not notify GDCA and relying parties promptly when information in the certificates is changed.
7. The private key is compromised, damaged, stolen, disclosed, and etc. due to not taking effective protection measures.
8. Subscribers continue to use the certificate 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.
9. The certificate has expired but is still in use.
10. The subscriber’s certificate information infringes upon the intellectual property rights of a third-party.
11. Using certificates beyond specified 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

如因下述情形而导致 GDCA 或订户遭受损失，依赖方应当承担赔偿责任：

1. 没有履行 GDCA 与依赖方的协议和本 CPS 中规定的义务；
2. 未能依照本 CPS 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. 在不合理的情形下信赖证书，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，但仍然信赖证书；
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。

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

1. Obligations defined in the CPS 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 CPS.
3. Trust certificates in unreasonable circumstances. For example, relying party still trusts the certificate with knowing that the certificate usage is beyond its scope or period or the certificate has or may have been stolen.
4. Relying party does not verify trust chains of the certificates.
5. Relying party does not check whether a certificate is revoked through querying CRL or OCSP.

9.10. 有效期限与终止 Term and Termination

9.10.1. 有效期限 Term

本 CPS 在发布日期零时正式生效，上一版本的 CPS 同时失效；本 CPS 在下一版本 CPS 生效之日或在 GDCA 终止电子认证服务时失效。

This CPS will enter into force at 12 o'clock midnight of the release date, and the last version CPS will become invalid. This CPS will become invalid when the next version CPS enters into force or the electronic certification services of GDCA are terminated.

9.10.2. 终止 Termination

在 GDCA 终止电子认证服务时，本 CPS 终止。

When GDCA terminates electronic certification services, this CPS is terminated.

9.10.3. 效力的终止与保留 Effect of Termination and Survival

本 CPS 终止后，其效力将同时终止，CPS 中的内容将视为无效使用，但对终止之日前发生的法律事实，CPS 中对各方责任的规定及责任免除仍然适用。

After the termination of this CPS, its effect will terminate at the same time. The contents in CPS will be considered as invalid. However, for the legal facts occurred before the date of termination, the regulation and the exemption of responsibilities defined in CPS for all parties are still applicable.

9.11. 对参与者的个别通告与沟通 Individual Notices and Communications with Participants

本 CPS 终止后，GDCA 将就文档失效的有关事项通知参与本机构电子认证活动的各有关当事人。

After the termination of this CPS, GDCA will notify all related parties who have participated in GDCA electronic certification activities about related matters on document expiration.

9.12. 修订 Amendments

9.12.1. 修订程序 Procedures 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 CPS，确保其符合国家法律法规和主管部门的要求及相关国际标准，符合 CP 的要求，符合认证业务开展的实际需要。

本 CPS 的修改和更新，由 CPS 编写小组提出修订报告，经 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 CPS 经过 GDCA 安全策略委员会批准后正式对外发布。

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

Revisions and updates of this CPS should be initiated by the CPS composition team and approved by GDCA Security Policy Committee. The revised CPS shall be officially released after being approved by GDCA Security Policy Committee.

9.12.2. 通知机制和期限 Notification Mechanism and Periods

修订后的 CPS 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 CPS, 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 implications.

9.12.3. 必须修改 OID 的情形 Circumstances under which OID Must be Changed

GDCA 负责确定 CPS 的修订是否需要修改 OID。

GDCA is responsible for determining whether an amendment to the CPS requires an OID change.

9.13. 争议处理 Dispute Resolution Provisions

GDCA、证书订户、依赖方等实体在电子认证活动中产生争议可按以下步骤解决：

1. 根据本 CPS 中的规定，明确责任方；
2. 由 GDCA 相关部门负责与申请人协调；
3. 若协调失败，再由有关法律部门进行裁决；
4. 任何与 GDCA 或授权机构就本 CPS 所涉及的任何争议提起诉讼的，受 GDCA 工商注册所在地人民法院管辖。

If GDCA, certificate subscribers, relying parties and other entities have disputes in the electronic certification activities, following steps can be taken for resolution:

1. Confirm the party to be held responsible according to this CPS;
2. GDCA's related departments are responsible for coordinating with the applicants;
3. If coordination fails, these parties should reach out to the legal authorities;
4. Prosecutions against GDCA or its authorized agencies over any disputes arising from this CPS should be governed by the people's court in the place where GDCA is registered.

9.14. 管辖法律 Governing Law

GDCA 的 CPS 受国家已颁布的《中华人民共和国电子签名法》和《电子认证服务管理办法》法律法规管辖。

The CPS of GDCA is governed by the law of "Electronic Signatures Laws of People's Republic of China" and the regulation of "Measures for the Administration of Electronic Certification Services" promulgated by the country.

9.15. 与适用法律的符合性 Compliance with Applicable Law

无论 GDCA 的证书订户、依赖方等实体在何地居住以及在何处使用 GDCA 的证书，

本 CPS 的执行、解释和程序有效性均适用中华人民共和国的法律。任何与 GDCA 或授权注册机构就本 CPS 所涉及的任何争议，均适应中华人民共和国法律。

Regardless of the place of residence for the subscribers, relying parties and other entities or place of use of the GDCA certificates, the execution, explanation and procedure should be compliant with laws of the People's Republic of China. Any disputes involved by GDCA and its RA in relation to this CPS should also be compliant with laws of the People's Republic of China.

9.16. 一般条款 Miscellaneous Provisions

9.16.1. 完整协议 Entire Agreement

GDCA 的 CPS 完整的文档结构包括：标题、目录、主体内容 3 部分。关于对目录和主体内容修改后的替代内容，将完全代替所有先前部分、并被放置在 GDCA 的网站中以供查阅和浏览。

Complete document structure of GDCA CPS includes 3 parts: titles, table of contents and main contents. Modified alternative content of the table of contents and the main contents will completely replace all previous parts. The previous parts would be placed at the GDCA web site for browsing.

9.16.2. 转让 Assignment

GDCA 声明，根据本 CPS 中详述的认证实体各方的权利和义务，各方当事人可按照法律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。

GDCA represents that, according to the rights and obligations of certification entity parties detailed in this CPS, 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 CPS 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 可以在最低必要的限度下修订该条款，使其继续有效，其余部分不受影响，GDCA 将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 将发送邮件至 question@cabforum.org，通知 CAB 论坛 CPS 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 业务操作的调整将不再继续适用。上述对业务操作进行的相关调整，对 GDCA 的 CPS 的修订，及向 CA/B 论坛的通知将在 90 天内完成。

In case any clause or provision of this CPS is held to be unenforceable or invalid due to any conflicts with the laws of any jurisdiction in which GDCA operates, GDCA may modify any conflicting clause or provision to the minimum extent necessary to make them continue to be valid, and other clauses and provisions will remain valid without being affected. GDCA will disclose the modified contents in this section.

GDCA will (and prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of any modified content in the CPS 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 will 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 CPS and a notice to the CA/Browser Forum, as outlined above, will 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)

GDCA 声明，若证书订户、依赖方等实体未执行 GDCA 的 CPS 中某项规定，不被认为该实体将来不执行该项或其他规定。

GDCA declares that, if the subscribers or relying parties did not execute any items within this CPS, it shall not be considered that they will not be executed in the future.

9.16.5. 不可抗力 Force Majeure

GDCA 不对因战争、瘟疫、火灾、地震和其他天灾等不可抗力的事件所造成本 CPS 规定担保责任的违反、延误或无法履行负责。

GDCA do not assume responsibilities for losses incurred by the violation, delay or inability to perform the CPS regulations due to the force majeure events like wars, epidemics, fires, earthquakes and other natural disasters.

9.17. 其他条款 Other Provisions

GDCA 对本 CPS 具有最终解释权。

GDCA has final interpretation rights to this CPS.

附录 1：根证书及中级 CA 证书信息

Appendix1: Certificate information of Root/Subordinate CA Certificates

Root/Subordinate CA Certificates	Information
GDCA TrustAUTH R5 ROOT	Country=CN Organization= GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. Common Name= GDCA TrustAUTH R5 ROOT Serial Number= 7d 09 97 fe f0 47 ea 7a Validity= November 26, 2014 to December 31, 2040 SHA1digest= 0f 36 38 5b 81 1a 25 c3 9b 31 4e 83 ca e9 34 66 70 cc 74 b4
GDCA TrustAUTH R4 EV SSL CA	See “GDCA EV CPS”
GDCA TrustAUTH R4 Plus EV CodeSigning CA	See “GDCA EV CPS”
GDCA TrustAUTH R4 CodeSigning CA2	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH R4 CodeSigning CA2 Serial Number= 1d a7 40 73 16 f6 1c 2b 17 47 d6 2f ea 8f 5b fe Validity：February 20, 2025 to February 10, 2040 SHA1 digest= 2f 4b 28 5d 33 b9 e4 ad e7 24 1d bb 29 63 de f0 3c 82 64 d2
GDCA TrustAUTH R4 OV SSL CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH R4 OV SSL CA Serial Number= 39 c0 77 fc 1e d6 15 e3 Validity：April 5, 2016 to December 31, 2030 SHA1 digest= c3 4a d6 45 d5 79 1c 5f 22 e7 33 d7 53 47 08 15 85 75 6c 2d
GDCA TrustAUTH R4 IV SSL CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH R4 IV SSL CA Serial Number= 28 34 52 f4 73 3f 26 a6 Validity：March 31, 2016 to December 31, 2030

	SHA1 digest= 78 ae a8 51 a3 1b 0f 04 9a f0 2c d0 f2 ad 91 40 60 4f a7 a3
GDCA TrustAUTH R4 DV SSL CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH R4 DV SSL CA Serial Number=76 39 e3 80 9c 62 1e 26 Validity：March 31, 2016 to December 31, 2030 SHA1 digest= 30 18 4a 5b 92 4e 67 9e 7a 91 32 93 17 d0 56 0f 58 7e 69 7b
GDCA TrustAUTH R4 CodeSigning CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH R4 CodeSigning CA Serial Number= 17 b3 ad d2 40 a3 b9 20 Validity：April 7, 2016 to December 31, 2030 SHA1 digest= fc 6d cb 06 a5 5b ff 76 83 64 27 5b 29 d6 4f 7c 3a a9 cf b4
GDCA TrustAUTH R4 TimeStamp CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH R4 TimeStamp CA Serial Number= 50 9e 8b 63 9c cf d5 fb ee b9 46 65 48 81 22 d1 Validity：June 29, 2022 to December 31, 2035 SHA1 digest= 86 e9 75 66 dc ec df d1 b1 a6 d2 e3 44 1d c4 a4 6e e6 34 4e
GDCA TrustAUTH R4 Generic CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH R4 Generic CA Serial Number= 28 35 6a 9c 70 b4 55 78 Validity：April 7, 2016 to December 31, 2030 SHA1 digest=6f ed 83 eb e1 83 cc 71 d0 ed e1 2a e8 77 e0 df 98 96 1f 24
GDCA TrustAUTH R4 Primer CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH R4 Primer CA Serial Number= 7a a7 21 5f 89 b7 19 02 Validity：March 31, 2016 to December 31, 2030

	SHA1 digest=14 c2 b3 3b bf 6e bd 84 fc a7 01 54 13 eb d0 43 3e 17 1a 98

Root/Subordinate CA Certificates	Information
数安时代 R5 根 CA 证书	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name=数安时代 R5 根 CA Serial Number= 2e d9 58 82 91 39 ad 07 Validity：March 31, 2016 to December 31, 2040 SHA1 digest= 23 eb 1b a4 64 71 a1 e7 e9 f2 db 57 01 fe f8 f2 f8 0c aa e9
数安时代 R4 EV 服务器证书 CA	See “GDCA EV CPS”
数安时代 R4 OV 服务器证书 CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name=数安时代 R4 OV 服务器证书 CA Serial Number= 78 b6 25 84 85 f2 84 9e Validity：March, 31, 2016 to December 31, 2030 SHA1 digest= 93 92 5b 05 17 30 05 86 fd 2c 45 eb 18 6e 00 9e b9 75 a5 d0
数安时代 R4 IV 服务器证书 CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name=数安时代 R4 IV 服务器证书 CA Serial Number= 13 28 8c d8 93 9c d0 49 Validity：March 31, 2016 to December 31, 2030 SHA1 digest= 10 b8 fb 9a d2 50 32 6a ee fb 05 ad da 9d 3a 2b bb bd 5d bf
数安时代 R4 DV 服务器证书 CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name=数安时代 R4 DV 服务器证书 CA Serial Number=6c 81 58 42 a9 55 70 3d Validity：March 31, 2016 to December 31, 2030 SHA1 digest=01 ad 04 cd e1 05 56 23 4a f6 6f a0 e6 64 f3 a6 18 80 4d f5
数安时代 R4 代码签名证书 CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd.

	Common Name=数安时代 R4 代码签名证书 CA Serial Number=6c 6c e2 6b 3e a8 4c 87 Validity：March 31, 2016 to December 31, 2030 SHA1 digest=4f be 54 bc 70 8e b1 2a 11 86 dd 79 aa ff e7 95 f8 ad c6 e9
数安时代 R4 普通订户证书 CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name=数安时代 R4 普通订户证书 CA Serial Number=7b 98 39 30 58 a0 9d 13 Validity：March 31, 2016 to December 31, 2030 SHA1 digest=07 33 29 cb 53 b1 86 36 25 38 1b fb 48 a0 43 a7 b1 fe 28 6f
数安时代 R4 基础订户证书 CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= 数安时代 R4 基础订户证书 CA Serial Number=68 f5 ae 07 7b cb da 8b Validity：March 31, 2016 to December 31, 2030 SHA1 digest=e5 da 52 2d 5f 38 7a 6e 72 49 5e 66 a4 be ba 0f 24 f2 59 dc

Root/Subordinate CA Certificates	Information
GDCA TrustAUTH E5 ROOT	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH E5 ROOT Serial Number= 1a f5 1f 4d 2c da bb 53 Validity：March 23, 2016 to December 31, 2040 SHA1 digest= eb 46 6c d3 75 65 f9 3c de 10 62 cd 8d 98 26 ed 23 73 0f 12
GDCA TrustAUTH E4 EV SSL CA	See “GDCA EV CPS”
GDCA TrustAUTH E4 OV SSL CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH E4 OV SSL CA Serial Number= 0f a7 49 2f 24 9b 14 de Validity：March 31, 2016 to December 31, 2030

	SHA1= 50 15 62 d8 1b a2 40 27 1b ee 06 d2 b3 7f 5b 35 cb 9d 8c b8
GDCA TrustAUTH E4 IV SSL CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH E4 IV SSL CA Serial Number= 51 ba 77 d9 8c b3 2a 3f Validity：March 31, 2016 to December 31, 2030 SHA1 digest= a8 45 2b fc 20 f9 de b6 9b 8b 3f 29 73 e0 a3 b3 6f 82 eb 5b
GDCA TrustAUTH E4 DV SSL CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH E4 DV SSL CA Serial Number=34 f2 54 c9 b2 fc 6a 6c Validity：March 31, 2016 to December 31, 2030 SHA1 digest= 8e 9b 9a db f5 ec c4 6b 05 76 82 2e de 5e 80 d1 57 6b 5d 7c
GDCA TrustAUTH E4 CodeSigning CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH E4 CodeSigning CA Serial Number=71 18 49 83 c1 22 58 ca Validity：March 31, 2016 to December 31, 2030 SHA1 digest= 10 6a 4e 5d ca 05 92 28 e4 ff 89 52 66 53 a4 64 7d 57 ee 63
GDCA TrustAUTH E4 Generic CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH E4 Generic CA Serial Number=05 ac ef 56 ff 70 b0 cb Validity：March 31, 2016 to December 31, 2030 SHA1 digest=fd 63 ba 6e e7 89 f6 0a 16 72 b5 b3 3a 29 7d 71 71 65 54 ee
GDCA TrustAUTH E4 Primer CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA TrustAUTH E4 Primer CA Serial Number=1d ad 3b b9 e6 71 7f e7 Validity：March 31, 2016 to December 31, 2030

	SHA1 digest=5f 42 a4 4d c8 ca 12 df ae 1c 29 92 1f 47 3e 3b be 8b d4 2c

Root/Subordinate CA Certificates	Information
ROOTCA（SM2）	Country =CN Organization = NRCAC Common Name= ROOTCA Serial Number= 69 e2 fe c0 17 0a c6 7b Validity：July 14, 2012 to July 7, 2042 SHA1 digest= 06 05 b6 26 16 8a 7a 78 5d 37 b9 78 b2 d7 21 05 85 d8 8f d9
GDCA TrustAUTH E1 CA	Country =CN Organization = GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. Common Name= GDCA TrustAUTH E1 CA Serial Number= 3e 7e 54 df dc 3f 77 bd 31 3b c8 31 99 21 8f d2 Validity：June 26, 2014 to June 21, 2034
GDCA SM2 ICA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA SM2 ICA Serial Number= 07 00 00 20 21 01 20 01 00 93 89 11 74 33 91 Validity：January 20, 2021 to December 31, 2033
GDCA Public SM2 CA1	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA Public SM2 CA1 Serial Number= 07 00 00 20 21 01 20 01 00 89 64 98 11 62 53 Validity：January 20, 2021 to December 31, 2033

Root/CA Certificate	Information
ROOTCA（RSA）	Country =CN Organization = OSCCA Common Name= ROOTCA Serial Number=6f 0c e9 52 69 c8 62 99 02 ff 63 a5 cc eb ed 3c Validity：August 28, 2005 to August 23, 2025

	SHA1 digest= db b8 44 23 c9 28 ab e8 89 d0 e3 68 fc 31 91 d1 51 dd b1 ab
GDCA TrustAUTH R2 CA	Country =CN Organization =GUANG DONG CERTIFICATE AUTHORITY CO.,LTD. Common Name= GDCA TrustAUTH R2 CA Serial Number=52 c4 67 59 4c d7 76 90 0d b8 8b 4c 58 01 eb 85 Validity：December 16, 2013 to December15, 2018 SHA1=c6 b2 19 eb 62 3d 68 cf ae 28 94 00 ad 2a b4 0a 28 d3 e3 1d

Root/Subordinate CA Certificates	Information
GDCA ROOT CA1（RSA）	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA ROOT CA1 Serial Number=2d ab 67 ea c5 5a c0 e4 Validity：June 11, 2017 to December 31, 2040 SHA1 digest= 0a 8f 00 29 ea 3c d0 51 a3 01 33 bd 7a a6 ec cf f8 ff ed c6
GDCA Public CA1	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA Public CA1 Serial Number= 27 5b 6e 83 2f 25 1c a7 b4 d1 a9 b6 af ff 92 5f Validity：July 4, 2024 to December 31, 2038 SHA1= 1a 46 3a de 53 25 aa 41 d4 ce c6 5a e7 16 bd 67 98 12 1f 31
GDCA Public CA2	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA Public CA2 Serial Number= 18 7d 43 6e 0e b2 80 3aValidity：February 25, 2021 to December 31, 2038 SHA1= d1 ab 2a ba 7e 4b 4d c6 df c4 8b a6 65 e1 e6 ad 74 0b 18 5b
GDCA HKMR OV CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA HKMR OV CA Serial Number= 2d 39 33 c0 39 8c de 65 Validity：September 12, 2018 to December 31, 2030 SHA1=01 96 64 be d9 eb cb e0 8f 19 39 79 bc f8 2d 10 52 50 ca c6
GDCA HKMR IV CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA HKMR IV CA Serial Number= 79 f1 1a 37 5f a5 58 12 Validity：September 12, 2018 to December 31, 2030

	SHA1= e9 2d ce 1f 67 00 78 06 8c ba d2 b0 b8 c9 4d a3 c6 cd f8 d6
GDCA RSA ICA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA RSA ICA Serial Number= 79 f1 1a 37 5f a5 58 12 Validity：January 20, 2021 to December 31, 2030 SHA1= e9 2d ce 1f 67 00 78 06 8c ba d2 b0 b8 c9 4d a3 c6 cd f8 d6
GDCA OTC CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name= GDCA OTC CA Serial Number= 4a 72 5a 2a ae ca 2d 05 Validity：August 22, 2018 to December 31, 2030 SHA1= 1d df ed 88 a6 2a e0 e6 9b 85 38 ad 2d 34 00 c3 23 0a 8c 45

附录 2：GDCA 电子认证业务规则修订记录表

Appendix 2: GDCA CPS Revision Records

内容 / 序号	修订章节	V6.2	V6.3
1	1.1.3 GDCA 证书层次架构 GDCA Certificate Hierarchical Architecture		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	5.7.1. 事故和损害处理程序 Incident and Compromise Handling Procedures		添加批量撤销相关内容。
9	6.7. 网络的安全控制 Network Security Controls		增加漏洞处理时限管理。
10	其他修订		调整个别措辞问题。

Content / No.	Sections Revised	V6.2	V6.3
1	1.1.3 GDCA 证书层次架构 GDCA Certificate Hierarchical Architecture		Add a new code signing Subordinate CA certificate.
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	5.7.1. 事故和损害处理程序 Incident and Compromise Handling Procedures		Add requirements related to mass revocation.
9	6.7. 网络的安全控制 Network Security Controls		Add management of vulnerability remediation timelines.
10	Other revisions		Adjust some wording issues.