数安时代科技股份有限公司

EV 证书策略

版本：2.0

发布日期：2020 年 5 月 31 日

Global Digital Cybersecurity Authority CO., LTD.

EV Certificate Policy (EV CP)

Version: 2.0

Release Date: May 31, 2020

目录

Contents

1. 引言 Introduction

1.1. 概述 Overview

1.1.1. 公司简介 Company Profile

数安时代科技股份有限公司（Global Digital Cybersecurity Authority Co., Ltd.，简称 GDCA 或“数安时代”,）原为“广东数字证书认证中心有限公司”，成立于 2003 年 3 月 6 日。2005 年 9 月，GDCA 依法通过了国家密码管理局和原国家信息产业部的资格审查，成为全国首批八家获得《电子认证服务许可证》（许可证号：ECP44010215007）的电子认证服务机构之一；2008 年 12 月，获得国家密码管理局颁发的《商用密码产品销售许可证》；2011 年 4 月，通过了国家密码管理局电子政务电子认证服务能力评估，获得《电子政务电子认证服务机构》（编号：A021）资格。2013 年，对电子认证服务系统进行 SM2 算法升级，并通过了国家密码管理局组织的安全性审查。2015 年，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 开始在新三板挂牌交易，股票简称：数安时代，股票代码：871932。

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

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

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”。

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

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

1.1.2. 证书策略 Certificate Policy (CP)

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

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

本 CP 遵循 CA/Browser Forum 制定的 Guidelines For The Issuance And Management Of Extended Validation Certificates（简称“EV Guidelines”）、Guidelines for the Issuance And Management of Extended Validation Code Signing Certificates（简称“EV Code Signing Guidelines”），即扩展验证证书指南（Guidelines for Extended Validation Certificates）的

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

This CP conforms to the latest version of the Guidelines for The Issuance and Management of Extended Validation Certificates (hereinafter referred to as “EV Guidelines”), Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates (hereinafter referred to as “EV Code Signing Guidelines”) namely the Guidelines for Extended Validation Certificates, and the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (hereinafter referred to as “Baseline Requirements”) formulated by CA/Browser Forum. Meanwhile, this CP meets the requirements of structure and content defined in Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, RFC3647 from The Internet Engineering Task Force, and GB 26855-2011-T Information Security Technology Public Key Infrastructure Certificate Policies and Certification Practice Statement Framework, and would make appropriate changes in accordance with Chinese laws and regulations together with operational requirements of GDCA.

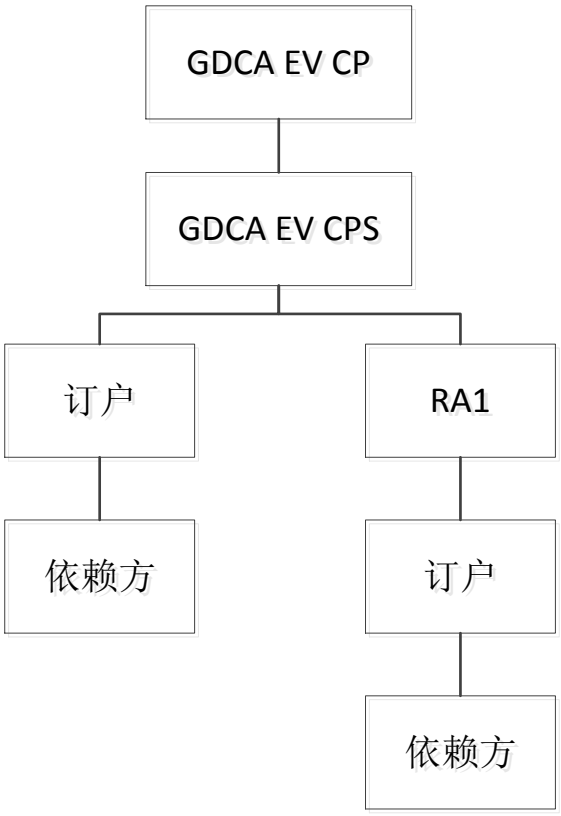
GDCA 作为一个证书服务机构（CA)，在本 CP 的约束下生成 EV 根证书和 EV CA 证书，签发订户证书。基于不同的类型和应用范围，作为证书持有人的订户可以使用证书进行网络站点安全保护、代码签名、邮件签名、文档签名、身份认证等不同的应用。依赖方依照本 CP 中关于依赖方的义务要求，决定是否信任一张证书。GDCA 的 EV 电子认证业务规则（EV CPS）接受本 CP 的约束，详细阐述了 GDCA 作为电子认证服务机构提供的证书、如何提供证书以及相应的管理、操作和保障措施。所有 GDCA 证书的订户及依赖方必须参照本 CP 及相关 EV CPS 的规定，决定对证书的使用和信任。

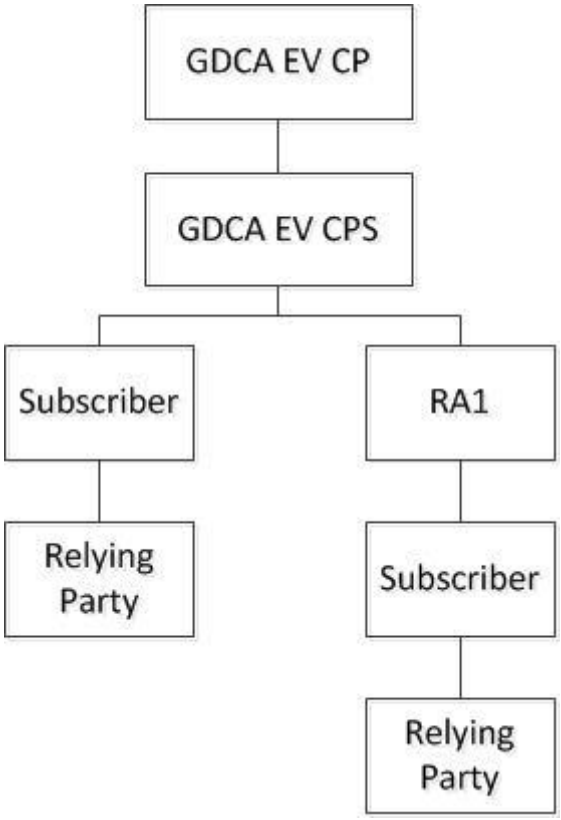
As a Certification Authority (CA), GDCA generates root and intermediate certificates, and issues certificates to subscribers under CP restrictions. Based on different types and application scope, digital certificates may be used by subscribers to process SSL, code signing, e-mail signing, document signing,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

1.1.3. GDCA 架构 GDCA Architecture

本 CP 是 GDCA 内 EV 证书的最高策略，GDCA 的证书服务机构（CA）按照本 CP 制定 EV CPS，RA 按照本 CP 及相关 CPS 进行证书服务申请鉴别，订户、依赖方及其他相关实体按照本 CP 及相关 EV CPS 决定对证书的使用、信任并履行相关的义务。

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



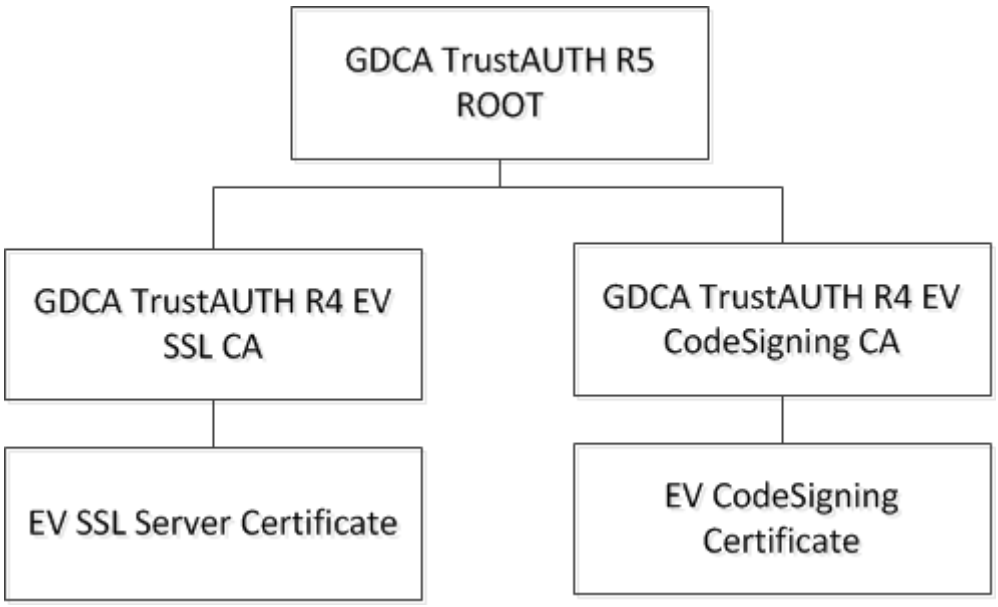


1.1.4. GDCA EV 证书层次架构 GDCA EV Certificate Hierarchical Architecture

GDCA 目前有 3 个 EV 根证书，分别为 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 3 EV root certificates, including GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA certificate, GDCA TrustAUTH E5 ROOT certificate. Each Root CA has Subordinate CAs to issue subscriber certificates. GDCA does not issue external Subordinate CA certificates.

1) GDCA TrustAUTH R5 ROOT



GDCA TrustAUTH R5 ROOT 证书的密钥长度为 4096-bit，下设 2 个中级 CA 证书，其中：（1）GDCA TrustAUTH R4 EV SSL CA 证书，密钥长度为 2048-bit，签发密钥长度为 2048-bit 的 EV SSL 服务器证书；（2）GDCA TrustAUTH R4 EV CodeSigning CA 证书，密钥长度为 2048-bit，签发密钥长度为 2048-bit 的 EV 代码签名证书。

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 EV 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。

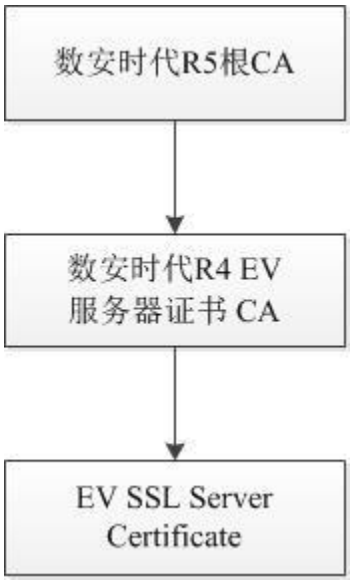
The length of GDCA TrustAUTH R5 ROOT certificate root key is 4096-bit. There are two Subordinate CAs under this root CA, including: (1) GDCA TrustAUTH R4 EV SSL CA is 2048-bit lengths and responsible for issuing 2048-bit EV SSL Server Certificates. (2) GDCA TrustAUTH R4 EV CodeSigning CA is 2048-bit lengths and responsible for issuing 2048-bit EV CodeSigning Certificates.

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

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

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

2) 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 1 个中级 CA 证书：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 2048-bit 的 EV SSL 服务器证书。

数安时代 R5 根 CA 证书将于 2040 年 12 月 31 日到期。

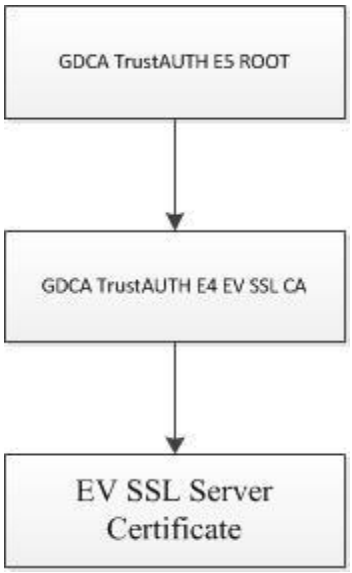
数安时代 R4 EV 服务器证书 CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

The length of 数安时代 R5 根 CA certificate root key is 4096-bit. There is one Subordinate CA under this root CA: 数安时代 R4 EV 服务器证书 CA is 2048-bit length and responsible for issuing 2048-bit EV SSL Server Certificates.

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.

3) GDCA TrustAUTH E5 ROOT



GDCA TrustAUTH E5 ROOT 证书证书的密码算法为 ECC，根密钥长度为 384-bit，下设 1 个中级 CA 证书：GDCA TrustAUTH E4 EV SSL CA ，密钥长度为 256-bit，签发密钥长度为 256-bit 的 EV SSL 服务器证书。

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。

The length of GDCA TrustAUTH E5 ROOT certificate root key is 384-bit using ECC algorithm. There is one Subordinate CA under this ROOT CA: GDCA TrustAUTH E4 EV SSL CA with 256-bit key length is responsible for issuing 256-bit EV SSL Server Certificates.

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 遵循 CA/浏览器论坛（CA/Browser Forum）发布的扩展验证证书指南的最新版本要求，以及 Baseline Requirements 进行签发和管理 EV 数字证书，定期查看其更新情况，并将持续根据其发布的版本进行修订 CP。如果本 CP 和 CA/浏览器论坛（CA/Browser Forum）发布的相关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 issues and manages the EV certificates based on the latest version of Guidelines for the Issuance and Management of Extended Validation Certificates, Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates, and the Baseline Requirements published by CA/Browser Forum. GDCA regularly checks the status on CA/Browser Forum's website and continuously revise this CP if there is any update. In the event that a discrepancy arises between interpretations of this document and CA/Browser Forum, the CA/Browser Forum shall govern.

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

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

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

本文档称作《数安时代科技股份有限公司 EV 证书策略 V2.0 版》（简称《GDCA EV CP V2.0》、本 CP）。有关本版本 CP 的修订信息请参考附录。本 CP 中为每类证书的证书策略项分配一个唯一的对象标识符，具体可参见本 CP 第 1.4.1.3 节。

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

This document is called "Global Digital Cybersecurity Authority CO., LTD. EV Certificate Policy V 2.0" (abbreviated as “GDCA EV CP V2.0” or “this CP”). Please refer to Appendix for detailed revisions of this version. Certificate policy for each kind of certificate is assigned a unique object identifier in this CP. Please refer to CP section1.4.1.3 for details.

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

1.3. PKI 参与者 PKI Participants

1.3.1. 电子认证服务机构 Certification Authorities

电子认证服务机构（Certification Authority，简称 CA）是颁发 EV 证书的实体。GDCA 是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定，依法设立的可信第三方电子认证服务机构。GDCA 通过给从事电子交易活动的各方主体颁发 EV 数字证书、提供证书验证服务等手段而成为电子认证活动的参与主体。

GDCA is a trusted third-party electronic authentication service authority established by law based on "Electronic Signature Law of the People's Republic of China" and "Measures for the Administration of Electronic Certification Services ". GDCA becomes a participant in electronic authentication activities by issuing EV certificate and providing certificate verification service to the parties who engage in electronic transactions.

1.3.2. 注册机构 Registration Authorities

注册机构（Registration Authority，简称 RA）代表 CA 建立起注册过程，确认 EV 证书申请者的身份，批准或拒绝 EV 证书申请者。

GDCA 作为 EV 证书的 CA 运营机构，自行担任 EV 证书 RA，不再另行设立 RA。

Registration Authorities (abbreviated as RA) set up registration process on behalf of CA, confirm the identity of applicant, and approve or reject the applicant.

As a CA operator of EV certificate, GDCA serves as RA of EV certificate by itself, and no longer to set up another RA.

1.3.3. 订户 Subscribers

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

Subscribers, the entities that receive certificates from CA, include individuals and organizations accepting certificates from GDCA. Subscribers and applicants would not always be the same; in this case, applicants need to ensure that they have obtained explicit and appropriate authorization. Individuals can be divided into a natural person and a person who belongs to an organization; Organization contains all kinds of government organizations, enterprises and institutions and other social groups. Usually, an organization has a legal personality or National Organization Code; for equipment certificates, due to the particularity of the entity contained in certificates, subscribers are usually organizations or individuals who own the equipment, and would assume the corresponding obligations.

GDCA 只对各类法人机构发放 EV 证书，不向自然人提供 EV 证书申请和签发服务。

GDCA only issues EV certificates to legal entities and doesn’t provide application and issuance services of EV certificate to natural person.

1.3.4. 依赖方 Relying Parties

依赖方是指信任并使用证书的实体。依赖方可以是证书订户，也可以不是证书订户。

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

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

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

1.3.5. 其他参与者 Other Participants

其他参与者是指为 GDCA 的电子认证活动提供相关服务的其他实体。

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

1.4. 证书应用 Certificate Usage

1.4.1. 适合的应用 Appropriate Certificate Uses

GDCA 签发的 EV 证书主要用于身份识别。凡是经过验证后确定是由 GDCA 签发的 EV 证书，均表明该证书中所包含的信息真实有效，并且已经通过了适当且可靠的身份鉴别程序。

EV certificate issued by GDCA is mainly used for identification. When the EV certificate is verified and confirmed the issuer is GDCA, it means that the information contained in the certificate is true and effective, and has passed the appropriate and reliable authentication procedure.

1.4.1.1. EV SSL 服务器证书 EV SSL Server Certificates

EV SSL 服务器证书用于验证证书中标识的网络主机服务器或互联网域名的身份，以及持有该网络服务器或互联网域名的法人机构身份。

GDCA 不签发通配符 EV SSL 服务器证书，除通配符域名外，EV SSL 服务器证书不限制域名的种类，如商业域名、政府域名等。

EV SSL server certificate is used for verifying the contents of certificates including: identity of network server, internet domain name and identity of organization who owns this server or domain name.

GDCA does not issue wildcard EV SSL server certificate. The types of domain names like business domain name or government domain name, except wildcard domain name, in EV SSL server certificates are not restricted.

1.4.1.2. EV 代码签名证书 EV CodeSigning Certificates

EV 代码签名证书用于验证证书中标识的软件代码提供方或发布方的身份。

EV CodeSigning certificate is used for verifying the identity of program provider or publisher.

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

在本 CP 中为每类 EV 证书的证书策略项分配一个唯一的对象标识符，具体如下：

EV SSL 服务器证书策略: 1.2.156.112559.1.1.6.1 及 2.23.140.1.1

EV 代码签名证书策略: 1.2.156.112559.1.1.7.1

GDCA assigns unique CP object identifiers of different EV certificate type in this CP, the regulation is as follows:

EV SSL server certificate policy: 1.2.156.112559.1.1.6.1 and 2.23.140.1.1

EV Code signing certificate policy: 1.2.156.112559.1.1.7.1

1.4.2. 限制的证书应用 Prohibited Certificate Uses

EV 证书除用于上述规定的范围外，不设计用于、不打算用于、也不授权用于危险环境中的控制设备，或用于要求防失败的场合，如核设备的操作、航天飞机的导航或通讯系统、空中交通控制系统或武器控制系统中，因为它的任何故障都可能导致死亡、人员伤害或严重的环境破坏。

EV 证书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，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，否则由此造成的法律后果由用户自己承担。

Except the scope of certificate usage specified above, EV certificate is not designed for, not intended for, and not authorized for control equipment in danger, or for the occasion prohibited to fail, such as operation of nuclear equipment, navigation or communication systems of shuttle, control systems of air traffic or weapon. These faults may lead to personal injury or serious environmental damage.

EV certificate is prohibited to be used in the circumstances that in violation of national laws, regulations or undermine national security; in addition, a certificate is prohibited to be used in business that involves criminal activities, or in business forbidden by laws. Otherwise, legal consequences caused by the above circumstances must be taken by the subscribers themselves.

1.5. 策略管理 Policy Administration

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

GDCA 安全策略委员会是 GDCA 电子认证服务所有策略的最高管理机构，负责制

定、维护和解释本 CP。

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

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

The committee consists of the relevant representatives with the right of decision-making from GDCA's management, administrative center, marketing center, technology center, customer service center, etc.

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 administrative center is responsible for external consulting services of this policy document and other related routines.

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：（国内地区）：95105813 或
  （国际地区）：+86-18929559132

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: 95105813 (China Olny) or
  +86 -18929559132 (For International Areas)

1.5.2.2. CPS 问题 CPS Related Issues

联系部门：GDCA 行政管理部门

联系人：王女士

邮件地址：gdca@gdca.com.cn

联系电话：+86 20-83487228

传真：+86 20-83486610

地址：中华人民共和国广东省广州市越秀区东风中路 448 号成悦大厦第 23 楼

邮编：510030

Contact Department: GDCA Administrative Department

Contact: Ms. Wang

E-mail: gdca@gdca.com.cn

Tel: +86 20-83487228

Fax: +86 20-83486610

Address: 23F, 448 Dongfeng Zhong Road, Guangzhou, Guangdong, the People's Republic of China

Postal Code: 510030

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

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

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

This CP and the corresponding modifications and version changes should be approved by GDCA security policy committee.

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

1.5.4. CP 批准程序 CP Approval Procedures

本 CP 由 GDCA 安全策略委员会主任及委员会常务秘书组织相关人员拟定文档，提交 GDCA 安全策略委员会批准审核。

After drafted by the team designated by GDCA security policy committee, the CP is submitted to GDCA security policy committee to audit.

1.5.5. CP 修订 CP Revision

GDCA 将对 CP 进行严格的版本控制，并由安全策略委员会负责相关事宜。

GDCA 根据国家的政策法规、技术要求、业务发展情况以及 CA/浏览器论坛（CA/Browser Forum）发布的扩展验证证书指南（Guidelines for Extended Validation

Certificates）以及 Baseline Requirements 的最新要求及时修订本 CP，CP 编写小组根据相关的情况拟定 CP 修订建议，提交 GDCA 安全策略委员会审核，经该委员会批准后，正式在 GDCA 官方网站上发布。

本 CP 至少每年修订一次。如果无内容改动，则递增版本号、更新发布时间、生效时间及修订记录。

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

This CP will be updated in accordance with the change of national policies and regulations, technical requirements, business development, as well as the latest requirements of the Guidelines for Extended Validation Certificates and the Baseline Requirements published by the CA/Browser Forum. The proposed suggestion of modification will be submitted by the team which is responsible for writing this CP based on relevant changes, then it would be reviewed by the GDCA Security Policy Committee. After approved by the committee, GDCA will publish the CP on the official website.

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

1.6. 定义和缩写 Definitions and Acronyms

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

术语	定义
GDCA 安全策略委员会	GDCA 认证服务体系内的最高策略管理监督机构和 CP 一致性决定机构。
电子认证服务机构	负责建立，签发，撤销及管理证书的某个机构。该术语适用于根 CAs 及中级 CAs。
注册机构	注册机构（Registration Authority，RA）负责处理证书申请者和证书订户的服务请求，并将之提交给认证服务机构，为最终证书申请者建立注册过程的实体，负责对证书申请者进行身份标识和鉴别，发起或传递证书撤销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。
证书	使用数字签名的电子文件，用于将公钥与身份绑定。
证书撤销列表	由签发证书的电子认证服务机构（CA）创建并进行数字签名，且定期更新的已撤销证书的带时间戳列表。
电子认证业务规则	构成证书建立，签发，管理及使用管理框架的一份文件。
域名	域名系统中分配至某个节点的标签。
完全限定域名	包括互联网域名系统中所有高级节点标签的域名。
在线证书状态协议	在线证书检查协议，可使依赖方应用软件判断某指定证书的状态。

私钥	由密钥对持有者严格保密的密钥对中的密钥，用于创建数字签名，及/或解密通过相应公钥加密的电子记录或文件。
公钥	密钥对中可由相应私钥持有者公开的密钥，可被某个依赖方使用，以核实与持有人相应私钥一并创建的数字签名，及/或可用于加密信息，以便仅相应私钥持有者可对此类信息进行解密。
公钥基础设施	一组包括硬件、软件、人员、流程、规则及责任的合集，用于实现基于公钥密码的密钥及证书的可信创建、签发、管理及使用的功能。
公共可信证书	由于其相应的根证书以信任锚的形式在广泛可用的应用软件中部署，从而可信的证书。
合格的审计师	符合本 CP 章节 8.3.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 CP and the decision-making agency pursuant to CP within the GDCA certification services system.
Certification Authority	An organization that is responsible for the creation, issuance, revocation, and management of certificates. The term applies equally to both Roots CAs and Subordinate CAs.
Registration Authority	A Registration Authority (RA) is responsible for processing service requests from certificate applicants and certificate subscribers, and submitting them to the certification authority for the final certificate applicant to establish registration process. RA is also responsible for identifying and verifying certificate applicants, initiating or transferring certificate revocation request, and approving certificate renewal or re-key request on behalf of the certification authority.
Certificate	An electronic document that uses a digital signature to bind a public key and an identity.
Certificate Revocation List	A regularly updated time-stamped list of revoked certificates that is created and digitally signed by the CA that issued the certificates.
Certification Practice Statement	One of several documents forming the governance framework in which certificates are created, issued, managed, and used.
Domain Name	The label assigned to a node in the Domain Name System.

Fully Qualified Domain Name	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
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 8.3. of this CP.
Relying Party	Any natural person or legal entity that relies on a valid certificate.
Subscriber	A natural person or legal entity to whom a certificate is issued and who is legally bound by a subscriber agreement.
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
WebTrust	The current version of CPA Canada’s WebTrust Program for Certification Authorities

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

CA	Certification/Certificate Authority	电子认证服务机构
CAA	Certification Authority Authorization	认证机构授权
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则

CRL	Certificate Revocation List	证书撤消列表
CSR	Certificate Signing Request	证书请求文件
DBA	Doing Business As	商业名称
DNS	Domain Name System	域名系统
EV	Extended Validation	扩展验证/增强验证
FIPS	(US Government) Federal Information Processing Standard	（美国政府）联邦信息处理标准
FQDN	Fully Qualified Domain Name	完全限定域名
GDCA	Global Digital Cybersecurity Authority CO., LTD.	数安时代科技股份有限公司
gTLD	Generic Top-Level Domain	通用顶级域名
IANA	Internet Assigned Numbers Authority	互联网编码分配机构
ICANN	Internet Corporation for Assigned Names and Numbers	互联网名字与编号分配机构
ISO	International Organization for Standardization	国际标准化组织
KM	Key Management	密钥管理
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
LRA	Local Registration Authority	本地注册机构
OCSP	Online Certificate Status Protocol	在线证书状态协议
OSCCA	State Cryptography Administration Office of Security Commercial Code Administration of China	中国国家商用密码管理办公室
PIN	Personal Identification Number	个人身份识别码
PKCS	Public KEY Cryptography Standards	公共密钥密码标准
PKI	Public Key Infrastructure	公钥基础设施
RA	Registration Authority	注册机构
RFC	Request For Comments	请求评注标准(一种互联网建议标准)
SSL	Secure Sockets Layer	安全套接字
TLS	Transport Layer Security	传输层安全

2. 发 布 与 信 息 库 责 任 Publication and Repository Responsibilities

2.1. 信息库 Repositories

GDCA 的电子认证信息库应包括以下内容：证书策略（CP）、电子认证业务规则（CPS）、证书、证书撤销列表（CRL）、证书在线状态查询（OCSP）等。

GDCA repositories should include the following: CP, CPS, certificate, CRL, OCSP, etc.

2.2. 信息的发布 Publication of 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 in formation of certificates and CRLs through GDCA's official website. Meanwhile, subscriber or relying party can get the current status of certificate instantly via OCSP service provided by GDCA.

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

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

GDCA 在订户证书签发或者注销时，通过官方网站自动将证书和 CRL 发布，发布周期为 24 小时，CRL 有效周期最长不超过 48 小时；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 and the CRLs are issued every 24 hours and are valid for no more than 48 hours. In particular, GDCA can choose time to release the certificates and CRL in case of an emergency. GDCA releases CRL of CA (ARL) once every year.

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

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

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

GDCA 通过网络安全防护、系统安全设计、安全管理制度确保只有经过授权的人员才能进行信息库的增加、删除、修改、发布等操作。

The information in GDCA repository is publicly available. Anybody can read the relevant information, and there are no restrictions on the read-only access of such information.

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

3. 身份标识与鉴别 Identification and Authentication

3.1. 命名 Naming

3.1.1. 命名类型 Type of Names

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

EV SSL 证书和 EV 代码签名证书命名规则和要求必须被记录在按照本 CP 制定的 CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第九部分的要求相一致。EV SSL 证书和 EV 代码签名证书的甄别名必须包含通用名（common name，CN=）内容，经过验证的通用名中应当包含域名、机构电子邮件地址、机构的合法名称等。

EV certificates issued by GDCA conform to X.509 standard and naming rules of Subject Distinguished Name assigned to certificate holder is in accordance with X.500 standard.

Naming rules and requirements of EV SSL certificate and EV code signing certificate must be stated in the CPS customized according to the CP, and in line with Section 9 requirements of Guidelines published by CA/ browser Forum at www.cabforum.org. Distinguish name of EV SSL certificate and EV code signing certificate must contain common name (CN=). Common name after verification should contain domain name, organization e-mail address, organization valid name, etc.

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

For EV SSL server certificate, all domain names are added as the Subject Alternative Name and a primary domain name shall be used as the Common Name.

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

订户证书所包含的命名应具有一定的代表性意义。订户证书中包含的主体识别名称，应当能够明确确定证书持有机构以及所要标识的网络主机服务器、互联网域名或软件发布者的身份，并且可以被依赖方识别。主体识别名称应当符合法律法规等相关规定的要求。

Names in subscriber certificates should have a significant meaning. Subject Distinguished Name in subscriber certificate shall definitely indicate the identities of certificate holders or specified internet servers, internet domain names or software publishers; it shall be identified by relying parties. The naming rules of Subject Distinguished Name shall meet the requirements of relevant laws and regulations.

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

订户不能使用匿名、伪名申请证书，证书中也不能使用匿名、伪名。

Subscriber cannot apply for certificate with anonymity or pseudonymity stated in this CP.

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

依 X.500 甄别名命名规则解释。

The format of DN conforms to X.500, and naming rules of DN are defined by GDCA.

3.1.5. 命名的唯一性 Uniqueness of Names

GDCA 应保证签发给某个订户的证书，其主体甄别名，在 GDCA 信任域内是唯一

的。但一个订户可以拥有两张或以上的使用同一个主题甄别名的证书。

Subject DN of certificate must be unique for different subscribers in GDCA trust domain. But a subscriber can hold more than one certificate using the same subject DN.

3.1.6. 命名纠纷的处理 Naming Dispute Processing

GDCA 不承担解决证书申请中关于命名纠纷的责任，发生纠纷时，订户应自行向司法机构或主管部门提出解决申请。

GDCA doesn't assume the responsibility of solving naming disputes during certificate application. When dispute is occurred, subscribers shall submit above issue to judicial institutions or administrative departments.

3.1.7. 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

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

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

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

在对机构身份进行鉴别时，鉴别流程应当明确记录在 EV CPS 中，并且要和 CA/

浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第十一部分的要求相一致。当证书中包含国际化域名（internationalized domain names，IDNs）时，应阻止国际化域名的同形异义欺骗（homographic spoofing）。

The identification procedures for organization identity authentication must be stated clearly in GDCA EV CPS and comply with the Section 11 of guidelines released by CA/Browser Forum at www.cabforum.org. Homographic spoofing should be prevented if the certificate contains internationalized domain names (IDNs).

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

GDCA 不接受个人用户的 EV 证书申请。

EV certificate does not accept individual application.

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

EV 证书中所有包含的订户信息都必须进行验证。

All information in EV certificate must be verified.

3.2.5. 授权确认 Validation of Authority

当机构订户授权经办人办理证书业务时，应当进行如下验证：

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

The following verification processes shall be taken when agents authorized by subscribers apply for certificates:

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

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

3.2.6. 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's 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.

3.2.7. 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，及伪造或更改可抗性进行评估，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。

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 13 个月，则 GDCA 可使用该数据及文件。

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

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

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

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

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

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

3.3.1. 常规密钥更新的标识与鉴别 Identification and Authentication for Routine Rekey

对于常规情况下的密钥更新，在 EV 证书到期前，订户应重新按照 CP 第 3.2 节关于证明私钥拥有方法的规定提交证书申请。

In general, subscriber should submit application for re-key according to CP section 3.2 on method to prove possession of private key before the expiration of EV certificate.

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 should make sure the encrypted documents or data have been decrypted before they apply for the secret key’s updating. GDCA shall not assume any responsibility due to failure of decryption by the renewal of the secret key.

3.4. 撤销后密钥更新的标识与鉴别 Identification and Authentication for Rekey After Revocation

EV 证书撤销后不能进行密钥更新。

Re-key/renewal after revocation is not permitted.

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

当订户提出 EV 证书撤销请求时，GDCA 将以初始注册时申请人提供的联络方式验证其请求。

When subscriber applies for EV certificate revocation, GDCA will contact with the subscriber according to the information recorded during initial registration procedure to verify the application.

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

4.1. 证书申请 Certificate Application

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

证书申请实体是具有独立法人资格的组织机构(包括行政机关、事业单位、社会团体和人民团体等)。

Certification application entities are organizations with independent legal person qualification (such as administrative organizations, institutions, social organizations, people's organizations and other organizations).

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

EV 证书注册操作应当明确记录在 EV CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第十部分的要求相一致。申

请者应事先了解订户协议、本 CP 及相应 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。

申请者应向 GDCA 递交 EV 证书申请表及相应证明文件，此行为即意味着申请者已经了解和接受上述内容。申请者应自行产生公私密钥对，产生 PKCS#10 证书请求文件并递交给 GDCA。

The EV certificate registration operation shall be stated clearly in GDCA EV CPS and be compliant with guidelines' Section 10 released by CA/Browser Forum at www.cabforum.org.Applicant should learn subscriber's agreement, provisions agreed in this CP and corresponding CPS and other files in advance. Especially, applicant should focus on related content about the certificate applicable scope, rights, obligations and guarantee.

Applicant should submit EV certificate application forms and corresponding documents to GDCA. All of above means that applicant has learned and accepted the contents. Applicants must generate public and private key pair by themselves and send a PKCS#10 certificate request file to GDCA.

4.2. 证书申请处理 Certificate Application Processing

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

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

在证书签发前，若 GDCA 根据 CP 第 3.2 节中指定来源获得的数据或证明文件的时间不超过 13 个月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 shall perform identity recognition and verification of identification over the subscriber according to the requirements of CP section 3.2.

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 thirteen months prior to issuing the certificate, and provided that no changes occurred to the documents and data within such time period.

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

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

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

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

如果符合下述条件，GDCA 可以批准证书申请：

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

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

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

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

如果发生下列情形，GDCA 应拒绝证书申请：

1. 该申请不符合本 CP 第 3.2 节关于订户身份的标识和鉴别规定；
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 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 shall refuse the certificate application:

1. The application does not meet the specifications of subscriber's identification and authentication in CP 3.2.
2. The applicant can't provide the required identity documents.
3. The applicant opposes or can't accept the relevant content or requirements of the subscriber's agreement.
4. The applicant has not paid or can't 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 the dispute, legal disputes or losses to the GDCA.

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

GDCA 的 EV 电子认证业务规则（CPS）应规定合理的证书申请处理时间。GDCA 应在 CPS 规定的时间内处理证书申请，无论是批准还是拒绝。

GDCA EV CPS should specify the processing period of certificate application. No matter approving or rejecting, GDCA should process certificate application within the period specified by GDCA EV CPS.

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

对于 GDCA 颁发的满足 CA/浏览器论坛 EV Guidelines、Baseline Requirements 要求的公共可信的 TLS/SSL 证书，GDCA 应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 应根据 RFC6844（经勘误表 5065 修订）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 不得签发对应的证书；若 CAA 记录中出现“iodef”标签，则 GDCA 应与申请者沟通后决定是否为其颁发证书。

GDCA 应以下列 CAA 记录查找失败情况作为可签发证书的条件：1）在非 GDCA 的基础设施中查询 CAA 记录失败；2）至少尝试过一次重新查找 CAA 记录；3）域名所在区域不存在指向 ICNNA 根区域的 DNSSEC 验证链。

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

GDCA shall process "issue", "issuewild", and “iodef” property tags according to RFC6844 as amended by Errata 5065: GDCA shall not issue corresponding certificates if the "issue", "issuewild" property tags do not contain “gdca.com.cn”. In case the property tag “iodef” is present in the CAA records, GDCA shall determine whether or not to issue certificates after communicating with the applicant.

GDCA shall treat a record lookup failure as permission to issue certificates if: 1) the failure is outside the GDCA's infrastructure; 2) the lookup has been retried at least once; and 3) the domain's zone does not have a DNSSEC validation chain to the ICANN root.

4.3. 证书签发 Certificate Issuance

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

根 CA 的证书签发应由 GDCA 授权的可信人员谨慎地发布直接指令，使根 CA 执行证书签名操作。

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

CA 将在证书申请被批准后生成并签发证书。CA 为申请人生成和签发的证书基于其在证书申请中被批准的信息。签发证书的操作应当明确记录在 EV CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 12 部分的要求相一致。

GDCA generates and issues certificates after approval of the application. CA generates and issues certificate for subscriber based on the information from certificate application form approved by GDCA. The operation of certificate issuance shall be stated clearly in GDCA EV CPS and be compliant with guidelines’ Section 12 released by CA/Browser Forum at www.cabforum.org.

4.3.2. CA 通知订户证书的签发 Notifications to Subscriber by the CA of Issuance of Certificate

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

GDCA will notify subscriber after issuing certificate. Subscriber can get the certificate via face- face, online download, or other methods agreed in advance by both sides.

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，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，并把证书通过邮件方式发送给订户，即代表订户接受了证书。
3. 订户反对证书或者证书内容的操作失败。

1. Subscribers can download certificates at the specific GDCA certificate service website. The download completeness indicates that subscribers have accepted the certificate.
2. GDCA's RA can download certificates for subscribers with the permission of subscriber. Then RA sends the certificates to subscriber through e-mail. It means the fact that subscriber has accepted this certificate.
3. Subscribers oppose the fail operation of certificate and its content

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

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

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

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

除证书订户外，GDCA 不需要通知其他实体证书的签发。

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

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

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

与证书中包含的公钥相对应的私钥只有在用户签署订户协议并接受证书后方可使用。使用证书符合订户协议、本 CP 和相关 CPS 的规定，并且必须与证书中密钥用途扩展项中定义的用途相一致。

订户应保护其私钥避免未经授权的使用，并且不再使用过期或被撤销的证书。私钥不得进行归档。

对于 EV 代码签名证书，不存在一个证书对应多个软件对象。

对于 EV SSL 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。

Only after subscribers sign the subscriber agreement and accept the certificate, the private key which is correspondent to the public key in the certificate can be used. The usages of the certificates must conform to the provisions of subscriber agreement, this CP and related CPS also must be compliant with the EKU defined in the certificate.

Subscriber shall protect his/her private key from unauthorized use. Subscribers should no longer use expired and revoked certificates. In addition, the private key should not be archived.

For EV CodeSigning certificates, a certificate cannot match multi-software at the same time.

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

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

当依赖方接收到加载数字签名的信息后，有义务进行以下确认操作：

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由 GDCA 所签发；
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。

以上任何一个环节失败，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。

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.

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

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

GDCA 不提供 EV 证书更新服务。

GDCA does not provide EV certificate renewal service.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

4.6.6. CA 对更新证书的发布 Publication of the Renewal Certificate by the CA

不适用。

Not applicable.

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

不适用。

Not applicable.

4.7. 证书密钥更新 Certificate Rekey

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

GDCA 的证书密钥更新包括但不限于以下情形：

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

1. 证书到期；
2. 基于技术、政策安全原因，GDCA 要求证书密钥更新。

1. The certificate expires.

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

4.7.2. 请求证书密钥更新的实体 Who May Request Certification of a New Public Key

请求证书密钥更新的实体为证书订户。

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

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

参照本 CP 第 3.3 节和本 CP 第 4.3 节的规定对证书密钥更新进行用户身份鉴别和识别以及证书签发。

The authentication and identification of subscriber for certificate rekey and the certificate issuance shall conform to CP section 3.3 and CP section 4.3.

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

同本 CP 第 4.3.2 节。

See CP section 4.3.2.

4.7.5. 构成接受密钥更新证书的行为 Conduct Constituting Acceptance of a Rekeyed Certificate

同本 CP 第 4.4.1 节。

See CP section 4.4.1.

4.7.6. CA 对密钥更新证书的发布 Publication of the Rekeyed Certificate by the CA

同本 CP 第 4.4.2 节。

See CP section 4.4.2.

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

同本 CP 第 4.4.3 节。

See CP section 4.4.3.

4.8. 证书变更 Certificate Modification

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

GDCA 不提供 EV 证书变更服务，如证书中包含的信息发生变更时应按照本 CP 第 4.9 节的规定撤销该证书，订户应按照本 CP 第 4.1、4.2、4.3、4.4 节的规定重新申请签发证书。

GDCA does not support modification of EV certificates. A certificate in which the information has been changed should be revoked according to CP section 4.9. Subscriber should re-apply the certificate according to CP section 4.1, CP section 4.2, CP section 4.3, and CP section 4.4.

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

不适用。

Not applicable.

4.8.3. 处理证书变更请求 Processing Certificate Modification Requests

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

4.9. 证书撤销和挂起 Certificate Revocation and Suspension

证书撤销和状态查询操作应当明确记录在 EV CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第 13 部分的要求相一致。

Certificate revocation and operation to query status shall be stated clearly in GDCA EV CPS and be compliant with guidelines' Section 13 published by CA/Browser Forum at www.cabforum.org.

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

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 或 IP 地址的域名授权或控制权的验证不应被依赖。

若出现以下情况中的一种或多种，CA 应在 24 小时之内撤销证书，且必须在 5 天之内撤销证书：

1. 证书不再符合 Baseline Requirements 第 6.1.5 节及第 6.1.6 节；
2. GDCA 获得了证书遭到误用的证据；
3. GDCA 获悉订户违反了订户协议、CP/CPS 中的一项或多项重大责任；
4. GDCA 获悉了任何表明 FQDN 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。
12. 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，证明生成私钥的方法有缺陷。

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 or IP address in the certificate should not be relied upon.

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 in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a domain name registrant's right to use the domain name, a relevant licensing or services agreement between the domain name registrant and the applicant has terminated, or the domain name registrant has failed to renew the domain name);
5. GDCA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name;
6. GDCA is made aware of a material change in the information contained in the certificate;
7. GDCA is made aware that the certificate was not issued in accordance with Baseline Requirements or GDCA's CP or CPS;
8. GDCA determines or is made aware that any of the information appearing in the certificate is inaccurate;
9. GDCA's right to issue certificates under the Baseline Requirements expires or is revoked or terminated, unless it has made arrangements to continue maintaining the CRL/OCSP repository ;
10. The fulfillment of the obligations in the CPS is delayed or encounters force majeure, such as natural disasters, computer or communications failures, changes of laws and regulations, government actions or other causes beyond the reasonable control, causing threats to the information of others; or
11. Subscribers fail to pay the service fees after GDCA performed the obligations of notifying the subscribers to pay;
12. 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), or if there is clear evidence that the specific method used to generate the private key was flawed.

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

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 私钥遭到了密钥损害，或不再符合密钥长度和公钥参数标准的要求；
2. GDCA 得到了证书遭到误用的证据；
3. GDCA 得知证书的签发未能符合，或中级 CA 未能符合适用的证书策略或认证业务规则；

4. GDCA 认为任何出现在中级 CA 证书中的信息为错误信息或具有误导性；
5. 中级 CA 由于任何原因停止运营；
6. 中级 CA 过期，或被撤销或被终止；

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 the requirements of the standards on key sizes and public key parameters;
2. GDCA obtains evidence that the certificate was misused;
3. GDCA is made aware that the certificate was not issued in accordance with or that subordinate CA has not complied with the applicable CP or CPS;
4. GDCA determines that any of the information appearing in the subordinate CA certificate is inaccurate or misleading;
5. The subordinate CA ceases operations for any reasons;
6. The subordinate CA expires or is revoked or terminated.

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

以下实体可以请求撤销一个订户证书：

1. GDCA；
2. 证书订户；
3. 法院、政府主管部门及其他的公权力部门；
4. 依赖方、应用软件提供商、防病毒机构或其他的第三方可以提交证书问题报告，告知 GDCA 有合理理由撤销证书。

The following entities can request revocation of a subscriber certificate:

1. GDCA;
2. Subscriber;
3. Court, government departments and other public power department;
4. 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. 证书撤销请求的处理程序 Procedure for Revocation Request

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

1. 订户向 GDCA 提交撤销申请表和身份证明材料，同时说明撤销原因；
2. GDCA 按照本 CP 第 3.4 节的规定进行证书撤销请求的鉴别；
3. GDCA 在接到撤销请求后的 2 个工作日内完成证书撤销；
4. GDCA 完成撤销后及时将其发布到证书撤销列表；
5. GDCA 通过电话、邮件等适当方式，通知订户证书被撤销及被撤销的理由;
6. GDCA 提供 7*24 小时的证书撤销申请服务。

1. Subscriber submits application form of revocation and documents of identity confirmation to GDCA. Meanwhile, subscriber should provide reasons of revocation.
2. GDCA makes authentication of certificate revocation request according to CP section 3.4.
3. GDCA completes certificate revocation within 2 working days after receiving revocation request.
4. After the completeness of revocation, GDCA releases it to CRL promptly.
5. GDCA notifies subscriber that the certificate was revoked and the revoked reason by appropriate means, such as telephone, mail, and etc.
6. GDCA offers 24x7 certificate revocation requests service.

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

1. 当 GDCA 有充分的理由确信出现本 CP 第 4.9.1.1 中节的情况时，可通过内部确定的流程撤销证书；
2. GDCA 提供 7*24 小时的证书问题报告和处理流程；
3. 当依赖方、司法机构、应用软件提供商、防病毒机构等第三方提请证书问题报告时，GDCA 应组织调查并根据调查结果来决定是否撤销证书；
4. GDCA 撤销订户证书后，通过适当的方式，包括电子邮件、电话等，告知订户证书已被撤销及撤销理由。

1. GDCA can revoke subscriber’s certificate with the occurrence of circumstances described in CP section 4.9.1 .1 after the approval of GDCA Security Policy Committee;
2. GDCA maintains a 24x7 certificate problems reporting and processing procedures;
3. GDCA will take actions to investigate the certificate problem reports submitted by relying

parties, judicial institutions, application software providers, anti-virus organizations and other third parties, and will decide whether or not to revoke the certificates based on the results of the investigation;

4. After the certificate revocation, GDCA or RA will use appropriate ways, including mail, phone etc. to notify the final subscriber that the certificate has been revoked and the reason why to be revoked.

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

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

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

4.9.5. CA 处理撤销请求的时限 Time Within Which CA Must Process the Revocation Request

GDCA 自接到撤销请求到完成撤销之间的间隔期限，不得超过 24 个小时。

The cycle of GDCA processes revocation request is 24 hours.

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

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

Relying parties must check the CRL published by GDCA before trusting a certificate to confirm the status of certificate.

4.9.7. CRL 发布频率 CRL Issuance Frequency

对于订户证书，GDCA 的 CRL 发布周期为 24 小时，CRL 有效周期最长不超过 48 小时，且 nextUpdate 字段的值不得超出 thisUpdate 值的 10 天以上。

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

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

For the subscriber certificates, GDCA shall update and publish certificate revocation list (CRL) every 24 hours, and the CRLs are valid for no more than 48 hours and the value of the nextUpdate field shall be no more than ten days beyond the value of the thisUpdate field.

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

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

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

一个 EV 证书从它被撤销到被发布到 CRL 上的滞后时间不能超过 24 小时。

CRL is effective after revocation request approved within 24 hours.

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

GDCA 应向证书订户和依赖方提供在线证书状态查询服务。OCSP 响应须符合 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 服务器的证书应包含一个 RFC6960 定义的类型为 id-pkix-ocsp-nocheck 的扩展项。

GDCA shall support OCSP responses for subscribers and the relying parties. The OCSP responses shall 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 shall contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

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

用户可以自由进行在线状态查询，GDCA 不得设置任何的读取权限。

GDCA 提供 Get 和 Post 两种方式的 OCSP 查询服务。

对于订户证书，GDCA 应至少每四天更新 OCSP 信息。OCSP 响应的最长有效期为 10 天。对于已经撤销的证书，立即更新 OCSP。

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

对于未签发的证书的状态查询请求，GDCA 不得返回“good”状态。

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

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

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

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

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

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

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

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

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

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

Except for the case described in CP section 4.9.1, when certificate key of subscriber or RA has been lost or probably lost, certificate revocation request must be made to GDCA immediately. If security of CA’s key (root CA or sub-CA key) is damaged or suspected damaged, GDCA should notify subscriber and relying party timely in reasonable time and appropriate way.

4.9.13. 证书挂起的情形 Circumstances for Suspension

GDCA 不支持证书挂起。

Not applicable.

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

GDCA 不支持证书挂起。

Not applicable.

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

GDCA 不支持证书挂起。

Not applicable.

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

GDCA 不支持证书挂起。

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

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

GDCA 不删除 OCSP 中的撤销记录。

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

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

GDCA does not remove the revocation records in the OCSP.

4.10.2. 服务可用性 Service Availability

证书状态服务必须保证 7X24 小时可用，且响应时间不得超过 10 秒。

证书状态服务的可用性应当明确记录在 EV CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第 13 部分的要求相一致。

Certificate Status Services must be available 24 × 7 without scheduled interruption, and the response time must be of ten seconds or less.

The availability of certificate service status shall be stated clearly in GDCA EV CPS and be compliant with guidelines' Section 13 published by CA/Browser Forum at www.cabforum.org.

4.10.3. 可选特征 Operational Features

参照本 CP 第 4.9.9、4.9.11 节 的规定。

See CP section 4.9.9, section 4.9.11.

4.11. 订购结束 End of Subscription

订户证书出现下列情形时表明订户的订购行为正式结束：

1. 证书到期后没有进行更新；
2. 证书到期前被撤销。

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

1. The certificate is not updated after expiration.
2. The certificate is revoked before expiration.

4.12. 密钥托管与恢复 Key Escrow and Recovery

4.12.1. 密钥托管与恢复的策略与行为 Key Escrow and Recovery Policy and Practices

GDCA 不得托管任何 EV 证书订户的私钥，因此也不提供密钥恢复服务。

GDCA does not escrow the private key of subscriber's EV certificate and thus does not provide key recovery services.

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

不适用。

Not applicable.

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

5.1. 物理控制 Physical Controls

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

GDCA 中心机房按照功能主要分为核心区、服务区、管理区、操作区、公共区五个区域。核心区是一个高性能电磁屏蔽室。其壳体是六面优质冷轧钢板，其中顶、墙板采用厚度为 2mm 的冷轧钢板，地板采用厚度为 3mm 的冷轧钢板。焊接工艺为 CO2 保护焊。玻璃是加厚的嵌有金属网的防弹玻璃。屏蔽门是手动锁紧屏蔽门。通风口是按屏蔽室规格配置蜂窝型通风波导窗。电源滤波器是单相高性能低泄漏滤波器。存放保密资料的密码柜必须放置在核心区。

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

5.1.2. 物理访问控制 Physical Access

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

定。

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

5.1.3. 电力与空调 Power and Air Conditioning

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

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

5.1.4. 防水 Water Exposures

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

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

5.1.5. 火灾防护 Fire Prevention and Protection

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

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

5.1.6. 介质存放 Media Storage

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

GDCA meets the security requirements for media storage, including fire-proof, water-proof, earthquake-proof, moisture-proof, corrosion-proof, pest-proof, static-proof, electromagnetic

radiation-proof, etc. Meanwhile, GDCA takes strict measures to prevent the media from unauthorized use and access.

5.1.7. 废物处理 Waste Disposal

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

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

5.1.8. 异地备份 Off-Site Backup

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

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

5.2. 程序控制 Procedural Controls

5.2.1. 可信角色 Trusted Roles

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

1. 密钥和密码设备的管理人员；
2. 系统管理人员；
3. 安全审计人员；
4. 业务管理人员及业务操作人员。

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

1. Administrator of key and password devices.
2. System administrator.

3. Security auditor.

4. Business administrator and business operator.

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

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

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

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

All 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

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

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

5. 安全审计

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

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

5.3. 人员控制 Personnel Controls

人员控制应当明确记录在EV CPS 中，并且要和CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 14.1 部分的要求相一致。

Personnel Controls shall be stated definitely in GDCA EV CPS and be accordance with guidelines Section 14.1 published by CA/Browser Forum at www.cabforum.org.

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

GDCA 对承担可信角色的工作人员的资格要求如下：

1. 具备良好的社会和工作背景；
2. 遵守国家法律、法规，服从 GDCA 的统一安排及管理；
3. 遵守 GDCA 有关安全管理的规范、规定和制度；
4. 具有良好的个人素质、修养以及认真负责的工作态度；
5. 具备良好的团队合作精神。
6. 无违法犯罪记录。

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。

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.

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

5.3.2. 背景调查程序 Background Check Procedures

GDCA 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。关键岗位必须进行全面调查。

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

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

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

Full review includes reviewing criminal records, social relation and social security besides basic review. Full reviews must be carried out for key roles.

调查程序包括：

a) 人事部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。
b) 人事部门通过电话、信函、网络、走访等形式对其提供的材料的真实性进行鉴定。
c) 用人部门通过现场考核、日常观察、情景考验等方式对其考察。根据考察的结果作出相应的安排。
d) 经考核，GDCA 与员工签订保密协议，以约束员工不许泄露 CA 证书服务的所有保密和敏感信息。同时，GDCA 还将按照本机构的人员管理相关条例对所有承担可信角色的在职人员进行职位考察，以便能够持续验证这些人员的可信程

度和工作能力。

Background review including: basic review and full review.

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

Full review includes reviews about criminal records, social relation and social security besides basic review.

The review procedure includes:

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

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

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

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

5.3.3. 培训要求 Training Requirements

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 安全管理机制；
- 岗位职责统一要求；
- 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、程序等。

Based on the position requirement of trusted role, GDCA shall arrange the corresponding pre-job training. The comprehensive training contents are as follows:

- GDCA operation system
- GDCA technology system
- GDCA security management mechanism

- Job responsibilities uniform requirement
- GDCA management policies, systems, measures, etc.
- The laws, regulations and standards, procedures of electronic certification service in China.

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

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

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

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

GDCA 应依据安全管理策略制定在职人员的工作岗位轮换周期和顺序。

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

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

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

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

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

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

For persons who do not belong to the GDCA but participate in the relevant works for GDCA businesses, such as business personnel of business branch organization, management personnel

and other independent contractors, GDCA has requirements are as follows:

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

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

GDCA 提供给内部员工的文件应包括培训材料和与员工工作相关文档。

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

5.4. 审计记录程序 Audit Logging Procedures

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

GDCA 应记录的事件包括但不限于：

1. 订户申请、注销、更新、挂失证书及 GDCA 撤销、冻结用户证书或用户申请恢复密钥等；
2. GDCA 成员的建立，变更，登陆，重新设置和变更口令，撤销特权，创建、更新和恢复密钥；
3. 连接失败；
4. 由 GDCA 进行读写操作；
5. 所有关联事件诸如证书撤销，安全政策修改以及有效使用，GDCA/Authority 软件起始与停止，使证书及证书链有效化，属性证书管理，更新订户，DN 变更，数据库及审计跟踪管理，证书生命周期管理及其它事件。

GDCA should record these events include but not limited to:

1. Certificate application, certificate suspension, certificate revocation and renew initiated by subscriber or by GDCA, subscriber applies for key recovery, etc.
2. Members of GDCA: Setup, change and login; Reset and alteration of password; revocation of privilege; Creation, renewal, and recovery of key.
3. Connection failure.
4. Read and write operations from GDCA.
5. All related events such as certificate revocation, security policy modification and effective use, start and end of GDCA/Authority software, making certificate and certificate chain effective, attribute certificate management, customer update, DN alteration, database and audit trail

management, certificate lifecycle management and other events.

5.4.2. 处理日志的频度 Frequency of Processing Log

GDCA 应定期检查审计日志，以便发现重要的安全和操作事件，对发现的安全事件采取相应的措施。

All the audit logs shall be checked by GDCA regularly in order to discover the significant security and operation events and take corresponding measures.

5.4.3. 审计日志的保留期限 Retention Period for Audit Log

GDCA 必须妥善保存电子认证服务的审计日志，保存期限为电子签名认证失效后十年。

GDCA must save electronic certification service audit logs properly. The preservation limitation period is ten years after the expiration of the electronic signature certification.

5.4.4. 审计日志的保护 Protection of Audit Log

所有的审计日志，应当采取严格的物理和逻辑访问控制措施，防止未经授权的浏览、修改、删除等。

All the audit logs should be handled with strict physical and logical access control measures to avoid unauthorized reading, modification and deletion, etc.

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

对审计日志的备份应该建立和执行可靠的制度，定期进行备份。

GDCA should set up and carry out the reliable system for backups of audit logs, and full backups are performed periodically.

5.4.6. 审计收集系统 Audit Collection System (Internal vs. External)

不适用。

Not applicable.

5.4.7. 对导致事件主体的通知 Notification to Event-Causing Subject

审计记录报告一个事件时，应通知引起该事件的个人、组织机构。

When audit record reports an event, GDCA shall notify individuals, organizations who cause this event.

5.4.8. 脆弱性评估 Vulnerability Assessments

根据审计记录，GDCA 应定期进行安全脆弱性评估，并根据评估报告采取补救措施。

GDCA shall conduct security vulnerability assessments regularly according to audit records and take remedial measures according to assessment reports.

5.5. 记录归档 Records Archival

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

需要归档的记录，除了本 CP 第 5.4.1 节规定的外，还需要对如下记录进行归档，包括：

1. 证书申请信息；
2. 证书签发过程中的支持文档。

In addition to the records need to be archived specified by CP section 5.4.1, the following records should be archived:

1. Information of certificate application.
2. Supporting documents of certificate issuance.

5.5.2. 归档记录的保留期限 Retention Period for Archive

GDCA 的 EV 电子认证业务规则（CPS）应规定合理的归档记录保留期限。

EV CPS of GDCA shall provide reasonable retention period for archive.

5.5.3. 归档文件的保护 Protection of Archive

应通过适当的物理和逻辑的访问控制方法保护归档数据，只有授权的可信人员允许访问归档数据，防止未经授权的浏览、修改、删除或其它的篡改行为。

All archive records shall take appropriate measures to control physical and logical access so that only trusted personnel can access records. Archive records shall be protected from the unauthorized browsing, modifying, deleting and other illegal operations.

5.5.4. 归档文件的备份程序 Archive Backup Procedures

对于系统生成的电子归档记录，应当定期进行备份，备份文件进行异地存放。

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。

Electronically archived records generated by the systems should be backed up weekly. The backup file should 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.

5.5.5. 记录时间戳要求 Requirements for Time-Stamping of Records

GDCA 的所有日志都有时间记录，均由操作人员手工记录或系统自动添加。

All the GDCA records are labelled with time, and the time will either be added manually by the operators or automatically by system.

5.5.6. 归档收集系统 Archive Collection System (Internal or External)

各自实体应在内部建设归档收集系统，包括 GDCA 和注册机构。

All the entities including GDCA and RA should construct internal archive collection system.

5.5.7. 获得和检验归档信息的程序 Procedures to Obtain and Verify Archive Information

GDCA 的安全审计员和业务管理员分别保留归档信息的 2 个拷贝。在获得完整档案信息时，须对这 2 个拷贝进行比较。

Security auditors and business administrators of GDCA retain 2 copies of the GDCA file information respectively. While obtaining the complete archived information, comparison of the 2 copies shall take place to confirm the integrity.

5.6. 密钥变更 Key Changeover

在 CA 证书到期时，GDCA 将对 CA 证书进行更新。只要 CA 密钥对的累计寿命没

有超过本 CP 第 6.3.2 节中规定的最大生命期，那么 CA 证书可以使用原密钥进行更新。否则需要产生新的密钥对，替换已经过期的 CA 密钥对。即使在密钥对生命期内，GDCA 也可以通过生成新密钥对的方式产生新的 CA 证书。在一个 CA 证书过期之前，密钥变更过程被启动，以保障这个 CA 体系中的实体从 CA 旧密钥对到新密钥对的平稳过渡。

When the certificate of CA expires, GDCA will renew the certificate of CA. As long as CA key pair does not exceed the maximum lifetime specified in Section 6.3.2, the certificate of CA could renew using original key. Otherwise, new key pair shall be generated to replace the expired key pairs of certificate of CA. Also, even in the key pair life cycle, GDCA could generate new certificate of CA by using new key pair. Before the certificate of former level CA expires, key changeover shall be performed to ensure that the entities in the CA system shall switch from original key pair to new key pair smoothly.

在生成新的 CA 密钥对时，必须严格遵守 GDCA 关于密钥管理的规范。新的密钥对产生时，GDCA 将签发新的 CA 证书，并及时进行发布，让订户和依赖方能够及时获取新的 CA 证书。

New CA key pair is generated according to the key management rules of GDCA strictly. While generating new key pair , GDCA shall issue and publish the new CA certificate timely, and it shall be available for subscriber and relying party to obtain new CA certificate.

CA 密钥更替时，必须保证整个证书链的顺利过渡。

Make sure that the entire certificate chain transits smoothly in CA key changeover.

5.7. 损害与灾难恢复 Compromise and Disaster Recovery

5.7.1. 事故和损害处理程序 Incident and Compromise Handling Procedures

GDCA 应制订各种事故处理方案和应急处理预案，规定相应的事故和损害处理程序。

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

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

如果出现计算机资源、软件和/或数据损坏的事件，GDCA 立即启动事故处理程序，如有必要，可按照灾难恢复计划实施恢复。

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 the intentional, man-made or natural disaster situation, 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 should 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 should be done by the system administrator.
6. While restore the GDCA business operator’s configuration file, it should be done by another GDCA security business operator or administrator.

当 CA 根私钥被攻破或泄露，GDCA 启动重大事件应急处理程序，由安全策略委员会和相关的专家进行评估，制定行动计划。如果需要注销 CA 证书，将会采取以下措施：

1. 告知依赖方和国家主管部门；
2. 发布证书注销状态到信息库；
3. 通过 GDCA 网站或其它通信方式发布关于注销 CA 证书的处理通报；
4. 产生新的根私钥，重新为订户签发证书。

When CA root private key has been damaged, missed, tampered or leaked, GDCA starts a major emergency treatment process, which is assessed by GDCA Security Policy Committee and the relevant experts to make a plan. If the CA certificate must be revoked, the following measures will

be taken:

1. Notify relying parties and state administrative department.
2. Publish certificate revocation status to repositories.
3. Publish handling notification about revoked certificates at GDCA website or by other communication methods.
4. Generate new root private key and re-issue certificate to subscriber.

5.7.4. 灾难后的业务存续能力 Business Continuity Capabilities After a Disaster

GDCA 在发生灾难后，应有如下几个方面的业务存续能力：

1. 在尽可能短的时间内恢复业务系统，最多不超过 48 小时；
2. 能够恢复客户信息；
3. 能够保证恢复后的运营场地符合安全要求；
4. 有足够的人员继续开展业务并且不违反职责分割的要求。

GDCA shall have the following continuity capabilities after a disaster:

1. Recover business system as soon as possible, not exceeding 48 hours.
2. Recover information of customers.
3. Ensure the operation site meets the security requirements after recovered.
4. There are enough employees to operate the business and not violating segregation of duties.

业务连续性的实施当明确记录在 EV CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 16 部分的要求相一致。

The implementation of Business Continuity shall be stated definitely in GDCA EV CPS and be accordance with guidelines Section 16 released by CA/Browser Forum at www.cabforum.org.

5.8. CA 或 RA 的终止 CA or RA Termination

当 GDCA 及其注册机构需要停止其业务时，必须严格按照《中华人民共和国电子签名法》、《电子认证服务管理办法》及相关法规中对认证机构终止电子认证服务的规定要求进行有关工作。

在 GDCA 终止前，必须：

1. 委托业务承接单位；
2. 起草 GDCA 终止声明；

3. 通知与 GDCA 终止相关的实体；
4. 关闭从目录服务器；
5. 证书注销；
6. 处理存档文件记录；
7. 停止认证中心的服务；
8. 存档主目录服务器；
9. 关闭主目录服务器；
10. 处理 GDCA 业务管理员和 GDCA 业务操作员；
11. 处理和存储敏感文档；
12. 清除 GDCA 主机硬件。

GDCA and its RA need to stop their business strictly under “electronic signature law on the People's Republic of China”, “electronic certification service management method” and relevant laws and regulations.

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. Process GDCA business administrator and GDCA business operator.
11. Process and store sensitive documents.
12. Remove GDCA mainframe hardware

当 RA 因故终止服务时，GDCA 将按照与其签订的相关协议处理有关业务承接事宜和其他事项。

When RA terminates its services, GDCA deals with all the relevant business in accordance with the agreements.

5.9. 数据安全 Data Security

数据安全应当明确记录在EV CPS 中，并且要和CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 16 部分的要求相一致。

Data security shall be stated definitely in GDCA EV CPS and be accordance with guidelines Section 16 released by CA/Browser Forum at www.cabforum.org.

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

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。

对于 EV SSL 订户证书，订户的密钥对由订户自己生成并保管。

对于 EV 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。

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 that approved and accepted by OSCCA and OSCCA implement a strict management of state's cryptographic products, GDCA only apply 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. Subscriber's key pair is generated by the key generation mechanisms embedded in his/her own server or other devices.

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 the CPS and follow the separation of roles principle. The procedures and operations related to key pair generation shall be recorded and archived.

For EV SSL certificates, subscribers' key pairs are generated and kept by the subscribers themselves.

For EV 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 thorugh secure channels.

6.1.2. 私钥传送给订户 Private Key Delivery to Subscriber

私钥由订户自行生成，不需要将私钥传递给订户。

Since the private key is generated by subscriber, GDCA dost not deliver private key to subscriber.

6.1.3. 公钥传送给证书签发机构 Public Key Delivery to Certificate Issuer

为了获得数字证书，最终订户和 RA 通过 PKCS#10 格式的证书签名请求信息或其它数字签名的文件包格式，以电子的方式将公钥提交给 GDCA 签发，这些请求或文件包的传送需要使用安全协议保护，比如安全套接层协议（SSL）。

In order to obtain a digital certificate, end subscriber and RA sends certification issuance request to GDCA electronically. The request contains public key for GDCA to issue the certificate. The request information is encoded as PKCS#10 or other packing format with digital signature. The transmission of these requests or file packages needs to use security protocol for protection, such as secure sockets layer protocol (SSL).

最终订户和 RA 通过 PKCS#10 格式的证书签名请求信息或其它数字签名的文件包格式，以电子的方式将公钥提交给 GDCA 签发，GDCA 在签发证书前验证所提交请求中的订户签名。

End subscriber and RA sends certification issuance request to GDCA electronically. The request contains public key for GDCA to issue the certificate. The request information is encoded as PKCS#10 or other packing format with digital signature.The subscriber's signature on the request is authenticated prior to issuing the certificate.

6.1.4. CA 公钥传送给依赖方 CA Public Key Delivery to Relying Parties

GDCA 应该通过安全可靠的途径将 CA 公钥传给依赖方，包括从安全站点下载、面对面的提交等方式。

GDCA 也需要通过目录发布其 CA 证书。

GDCA shall use secure and reliable way to deliver CA public key to relying party, including download from security site, face to face submission, etc.

GDCA also publishes CA certificate through server directory.

6.1.5. 密钥的长度 Key Length

GDCA 支持的 RSA 密钥长度至少是 2048 位，支持的 ECC 密钥长度至少为 256 位。

密钥长度应当明确记录在 EV CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 9.5 部分的要求相一致。

The key size of RSA is no less than 2048 bits. The key size of ECC is no less than 256 bits.

Key sizes shall be stated definitely in GDCA EV CPS and be accordance with guidelines Section 9.5 released by CA/Browser Forum at www.cabforum.org.

6.1.6. 公钥参数的生成和质量检查 Public Key Parameters Generation and Quality Checking

公钥参数必须使用国家密码主管部门批准许可的加密设备和硬件介质生成，例如加密机、加密卡、USB Key、IC 卡等生成和选取，并遵从这些设备的生成规范和标准。GDCA 认为这些设备和介质内置的协议、算法等已经具备了足够的安全等级要求。

对于参数质量的检查，同样由通过国家密码主管部门批准许可的加密设备和硬件介质进行，例如加密机、加密卡、USB Key、IC 卡等。

Public key parameters must be generated in encryption equipment and hardware medium approved and permitted by State Cryptography Administration, such as encryption machine, encryption card, USB Key, IC card, and follow generation norms and standards of these devices. Of course, 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 State Cryptography Administration, such as encryption machine, encryption card, USB Key, IC cards.

6.1.7. 密钥使用目的 Key Usage Purposes (as per X.509 v3 Key Usage Field)

GDCA 签发的 X.509v3 证书包含了密钥用法扩展项，其用法与 RFC 5280 标准 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008) 相符。如

果 GDCA 在其签发证书的密钥用法扩展项内指明了用途，证书订户必须按照该指明的用途使用密钥。参见本 CP 第 7.1.2 节。

X.509v3 certificates issued by GDCA contain key usage extension, which matches RFC 5280 standard (Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002). If GDCA specifies the usage in key usage extension in the issued certificate, the subscribers must use the key according to the specified usage. See CP section 7.1.2.

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

认证机构必须通过物理、逻辑和过程控制的综合实现来确保 CA 私钥的安全。订户协议会要求证书订户采取必要的预防措施防止私钥的丢失、泄露、更改或未经授权的使用。

Physical, logical and process control approaches must be synthetically used to ensure the security of CA's private keys. Subscriber agreement will require certificate subscriber to take necessary measures to prevent the loss, leak, changes, or unauthorized use of the private key.

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

GDCA 必须使用国家密码管理部门认可、批准的硬件密码模块生成根 CA、签发证书的 CA 和其他 CA 密钥对，并存储相关 CA 私钥。CA 系统的密码模块符合 FIPS 140-2 第三级别的技术要求，订户使用的密码模块符合 FIPS 140-2 第二级别的技术要求。

GDCA must use the hardware cryptographic module approved and permitted by State Cryptography Administrator to generate the key pair of root CA, issuing CA, other CA and store relevant private key of CA. The cryptographic module of the CA system meets the FIPS 140-2 Level 3 technical requirements, and the cryptographic modules of the subscribers conform to the FIPS 140-2 level 2 technical requirements.

6.2.2. 私钥多人控制（m 选 n）Private Key (n out of m) Multi-Person Control

认证机构必须通过技术及过程上的控制机制来实现多名可信人员共同参与 CA 加密设备的操作。技术上的控制可使用“秘密分割”技术，即将使用一个 CA 私钥时所需的激活数据分成若干个部分，分别由多名可信人员持有。如果为一个硬件密码模块的秘密分割总数为 m，那么必须有超过 n 个的可信人员才能激活储存在密码模块中的 CA 私

钥。在这里 m 不小于 5，n 不小于 3。

CA must use technology and process control mechanisms to achieve multi-reliable personnel jointly participate in the operation of CA encryption equipment. The “Secret Sharing “technology is adopted, namely, the activated data required in operating the private key of CA is split into the several parts and the parts are held by several trusted personnel. If hardware cryptography module’s secret division amount ism, then at least the number of n of trusted personnel must be required to activate CA private key stored in this cryptography module. It notes that m is not less than 5, n is not less than 3.

6.2.3. 私钥托管 Private Key Escrow

不适用。

Not applicable.

6.2.4. 私钥备份 Private Key Backup

为了保证业务持续开展，GDCA 必须创建 CA 私钥的备份，以备灾难恢复使用。私钥备份以加密的形式保存在硬件密码模块中。存储 CA 私钥的密码模块应符合 CP 第 6.2.1 节的要求并存放在保险柜中。CA 私钥复制到备份硬件密码模块中要符合 CP 第 6.2.6 节的要求。

In order to ensure ongoing operations, GDCA must create backup of the CA private key for disaster recovery. Such keys are stored in encrypted form in hardware cryptographic modules and associated key storage devices Backup of the private key in encrypted form is stored in the hardware cryptographic module, and cryptographic modules used for CA private key storage meet the requirements of section 6.2.1 and are stored in safety box. CA private key is copied to backup for hardware cryptographic module to meet the requirements of section 6.2.6.

6.2.5. 私钥归档 Private Key Archival

在 CA 私钥到期后，必须使用满足 CP 第 6.2.1 节要求的硬件密码模块归档保存至少 5 年。归档期限结束后，对 CA 私钥的销毁应符合 CP 第 6.2.10 节的规定。

After the expiration of private key, GDCA must use the hardware cryptographic module specified by CP section 6.2.1 to archive and store at least 5 years. After the expiration of archival, the destruction of private key shall meet the provision of CP section 6.2.10.

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

CA 的私钥，GDCA 应严格按照根密钥管理规范进行备份，除此之外的任何导入导出操作将不被允许。当 CA 密钥对备份到另外的硬件密码模块上时，以加密的形式在模块之间传送，并且在传递前要进行身份鉴别，以防止 CA 私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

GDCA private key backup is run strictly in accordance with procedure and strategies specified by GDCA, in addition, any import and export operations are not be allowed. When CA key pair is backed up to another hardware cryptographic module, by the way of the encrypted form to transmit between the modules, and made a authentication before the transmitting to prevent the CA private key from being lost, stolen, modified, disclosure non-authorized, used unauthorized.

GDCA 不提供订户私钥从硬件密码模块中导出的方法，也不允许如此操作。对于存放在软件密码模块中的私钥，如果订户愿意并且自行承担相关风险，订户可自主选择导入导出的方式，操作时需要采用口令保护等授权访问控制措施。

GDCA does not provide the export of subscriber’s private key from hardware cryptographic module and allow this operation. As for the private key stored in software cryptographic module, and if subscriber is willing to bear the relevant risks, subscriber can choose the way of import and export with access control such as password, etc.

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

CA 系统的私钥必须以密文的形式存放在国家密码主管部门批准和许可的硬件密码模块中。硬件密码模块至少符合 FIPS 140-2 三级标准或同等级安全水平。

用于安全存储 EV 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 private key of CA systems in encrypted form must be stored in Hardware Security Module approved and permitted by OSCCA, and hardware cryptographic module at least meets the FIPS 140-2 level 3 standards or equivalent security levels.

The hardware cryptographic module used to store the private keys of the EV code signing certificates at least meets the FIPS 140-2 level 2 standards or equivalent level of security.

6.2.8. 激活私钥的方法 Method of Activating Private Key

CA 的私钥存放于硬件密码模块中，其激活数据按照 CP 第 6.2.2 节进行分割，并且保存在 IC 卡等硬件介质中，必须由 m 选 n 的方式分别输入激活数据才能激活私钥。

The private key of CA shall be saved in hardware cryptographic module, and its activation data shall be spilt in accordance with Section 6.2.2, and be saved in the hardware media such as IC card. The private key must be activated through entering the data using n out of m.

6.2.9. 冻结私钥的方法 Method of Deactivating Private Key

对于 CA 私钥，当存放私钥的设备断电，私钥就被冻结。

The private key will be deactivated when its storage device powers off.

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

私钥不再使用、不需要保存时，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授权使用。

When private key is no longer used and do not need to be saved, it shall be destroyed so as to avoid loss, stealing and disclosure or unauthorized usage.

CA 私钥，在生命周期结束后，需将 CA 私钥的一个或多个备份进行归档，其他的 CA 私钥备份被安全销毁。归档的 CA 私钥在其归档期限结束时需在多名可信人员参与的情况下安全销毁。CA 私钥存放在硬件加密卡中，CA 私钥的销毁必须通过将 CA 私钥从加密卡中彻底删除或将加密卡初始化的方式销毁。

After the termination of lifetime, GDCA need archive one or more backup of CA private key and securely destroy other CA private key backup. The archived private key of CA shall be destroyed by multiple Trusted Persons during its archiving period. The CA private key is stored in the hardware encryption card, the destruction of CA private key must use the method that the CA private key is deleted from the encryption card completely or is destroyed with encryption card initialization.

6.2.11. 密码模块的评估 Cryptographic Module Capabilities

GDCA 使用国家密码主管部门批准和许可的密码产品，接受其颁发的各类标准、规范、评估结果、评价证书等各类要求，并参照 CNS 15135、ISO 19790 或 FIPS 140-2 等级 3 相关规定，GDCA 可根据产品性能、工作效率、供应厂商的资质等方面的条件，选择所需要的模块。

GDCA uses the products approved and permitted by state cryptography department, accepts various standards, specifications, assessment, evaluation certification and other requirements published by state cryptography department, and follows the related specifications of CNS 15135, ISO19790 or FIPS 140-2 level 3. GDCA selects the module according to product performance, efficiency, suppliers' qualifications and other aspects.

6.3. 密钥对管理的其他方面 Other Aspects of Key Pair Management

6.3.1. 公钥归档 Public Key Archival

必须归档 CA 和最终订户证书，归档的证书可存放在数据库中。

GDCA must archive CA and end subscriber certificate, and archived certificate can be stored in database.

6.3.2. 证书操作期和密钥对使用期限 Certificate Operational Periods and Key Pair Usage Periods

证书有效期应当明确记录在 EV CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 9.4 部分的要求相一致。

Certificate validation period shall be stated definitely in GDCA EV CPS and be accordance with guidelines Section 9.4 released by CA/Browser Forum at www.cabforum.org.

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 surpass the validity period of certificate. However, in order to ensure signature information can be verified within the certificate validity period, the public key can be used surpass the validity period of certificate.

For the encryption certificate, its public key can only be used for encryption within the validity period of certificate and not be used surpass the validity period of certificate. However, in order to ensure information encrypted can be used to unlock the information within the validity period of certificate, the private key can be used surpass the validity period of certificate.

另外需注意的是无论是订户证书还是 CA 证书，证书到期后，在保证安全的情况下，允许使用原密钥对对证书进行更新。但是密钥对不能无限期使用。

In addition, after the expiration of certificate, under the circumstances of ensuring security, original key pair can be used to update the certificate. But the key pair can't be used indefinitely.

对于不同的证书，其密钥对允许通过证书更新的最长使用期限如下：

1. 对于 RSA4096 位 CA 证书，其密钥对的最长允许使用年限是 30 年
2. 对于 RSA2048 位 CA 证书，其密钥对的最长允许使用年限是 27 年
3. 对于 ECC384 位 CA 证书，其密钥对的最长允许使用年限是 30 年
4. 对于 ECC256 位 CA 证书，其密钥对的最长允许使用年限是 27 年
5. 对于 RSA2048 位 EV 代码签名证书，其密钥对的最长允许使用年限是 39 个月
6. 对于 RSA2048 位 EV SSL 服务器证书，其密钥对的最长允许使用年限是 825 天
7. 对于 ECC256 位 EV SSL 服务器证书，其密钥对的最长允许使用年限是 825 天

从 2020 年 9 月 1 日起，SSL/TLS 服务器证书密钥对的最长允许使用期限是 398 天，可少于 398 天。

For different certificates, the maximum usage period of the key pair can be obtained via certificate renewal are as following:

1. For RSA 4096-bit CA certificate, the maximum usage period of the key pair is 30 years.
2. For RSA 2048-bit CA certificate, the maximum usage period of the key pair is 27 years.
3. For ECC 384-bit CA certificate, the maximum usage period of the key pair is 30 years.
4. For ECC 256-bit CA certificate, the maximum usage period of the key pair is 27 years.
5. For RSA 2048-bit EV Code Signing certificate, the maximum usage period of the key pair is 39 months.
6. For RSA 2048-bit EV SSL server certificate, the maximum usage period of the key pair is 825 days.
7. For ECC 256-bit EV SSL server certificate, the maximum usage period of the key pair is 825 days.

For the SSL/TLS Certificates issued on or after September 1, 2020, the maximum usage period of the key pair is 398 days or less.

6.4. 激活数据 Activation Data

6.4.1. 激活数据的产生和安装 Activation Data Generation and Installation

CA 私钥的激活数据，必须按照关于密钥激活数据分割和密钥管理办法的要求，严格进行生成、分发和使用。

Activation data of CA private key must be generated, distributed and used strictly according to the requirements which are related to the segmentation of key activation data and key management.

6.4.2. 激活数据的保护 Activation Data Protection

对于 CA 私钥的激活数据，必须通过秘密分割将分割后的激活数据由不同的可信人员掌管，而且掌管人员必须符合职责分割的要求，签署协议确认他们知悉秘密分割掌管者责任。

Activation data of CA private key must be separated in reliable way and kept by different trusted personnel. Administrator must meet their requirements of responsibility division. The responsibilities of key sharing holders should be confirmed by signing related agreements.

6.4.3. 激活数据的其他方面 Other Aspects of Activation Data

不做规定。

Not applicable.

6.5. 计算机安全控制 Computer Security Controls

6.5.1. 特别的计算机安全技术要求 Specific Computer Security Technical Requirements

GDCA 系统的信息安全管理，按照国家密码管理局公布的《证书认证系统密码及其相关安全技术规范》、工业和信息化部公布的《电子认证服务管理办法》，参照 ISO27001 信息安全标准规范以及其他相关的信息安全标准，制定出全面、完善的安全管理策略和制度，在运营中予以实施、审查和记录。主要的安全技术和控制措施包括：身份识别和验证、逻辑访问控制、物理访问控制、人员职责分权管理、网络访问控制等。

Information security management of GDCA certification system meets "Specifications Related

Security Technology Certificate Authentication System" published by OSCCA, "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.

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。

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。

Strict security controls ensures that the system of CA software and data files is secure and reliable without unauthorized access.

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.

系统安全应当明确记录在 EV CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 16.5 部分的要求相一致。

System security shall be stated definitely in GDCA EV CPS and be accordance with guidelines Section 16.5 released by CA/Browser Forum at www.cabforum.org.

6.5.2. 计算机安全评估 Computer Security Rating

GDCA 的认证系统，通过了国家密码管理局的安全性审查。

GDCA certification systems pass the security review of OSCCA.

6.6. 生命周期技术控制 Life Cycle Technical Controls

6.6.1. 系统开发控制 System Development Controls

GDCA 的软件设计和开发过程遵循以下原则：

1. 第三方验证和审查；
2. 安全风险分析和可靠性设计；

同时，GDCA 的软件开发操作规范，参考 ISO15408 的标准，执行相关的规划和开发控制。

Software design and development of GDCA process follows principles:

1. Verification and review of third-party
2. The security risk analysis and reliability design

The operation specifications of software development, which refer to ISO15408 standard, implement relevant plan and development control.

6.6.2. 安全管理控制 Security Management Controls

GDCA 认证系统的信息安全管理，严格遵循国家密码主管部门的有关运行管理规范进行操作。

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 through rigorous testing and verifying. Any modifications and upgrades will be recorded for reference and made for version control, functional test and record. GDCA also carries out regular and irregular inspection and test for certification system.

GDCA uses the flexible management system to control, monitor system configuration and prevent unauthorized modification.

硬件设备由采购到接收时，会进行安全性的检查，用来识别设备是否被入侵，是否存在安全漏洞等。加密设备的采购和安装必须在更加严格的安全控制机制下，进行设备的检验、安装和验收。

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。

为了确保网络安全，GDCA 认证系统安装部署了入侵检测、安全审计、防病毒和网管系统，并且及时更新防火墙、入侵检测、安全审计、防病毒和网管系统的版本，以尽可能的降低来自于网络的风险。

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

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.

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 the system time of GDCA's operation system synchronizes with this time stamp service through Network Time Protocol (NTP).

7. 证书、证书撤销列表和在线证书状态协议 Certificate, CRL, and OCSP Profiles

7.1. 证书描述 Certificate Profile

GDCA 证书遵循 ITU-T X.509v3（1997）：信息技术-开放系统互连-目录：认证框架（1997 年 6 月）标准和 RFC 5280：Internet X.509 公钥基础设施证书和 CRL 结构（2008 年 5 月）。

The format of GDCA certificates conforms to national standard, i.e. ITU-T X.509 V3 (1997): Information Technology - Open Systems Interconnection - the Directory - Authentication Framework (June 1997) recommendation by ITU-T and RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (May 2008).

GDCA 通过 CSPRNG 生成大于 0 且长度为 64 位的非序列性的证书序列号。

GDCA generates non-sequential certificate serial numbers greater than zero containing 64 bits of output from a CSPRNG.

EV 证书至少包含基本的 X.509 v1 域，其规定值或值的限制如下表所描述。

Certificate contains at least basic X.509 v1 domain, and its specified value or limited value is described as follow:

表-EV 证书结构的基本域

域	值或值的限制
版本	指明 X.509 证书的格式版本，值为 V3
序列号	证书的唯一标识符
签名算法	签发证书时所使用的签名算法（见 CP 第 7.1.3 节）
签发者 DN	签发者的甄别名
有效起始日期	基于国际通用时间(UTC)，和北京时间同步，按 RFC 5280 要求编码
有效终止日期	基于国际通用时间(UTC)，和北京时间同步，按 RFC 5280 要求编码。 有效期限的设置符合 CP 第 6.3.2 节规定的限制。
主题 DN	证书持有者或实体的甄别名，包括： CN、OU、O、streetAddress、postalCode、L、ST、C、serialNumber、businessCategory、1.3.6.1 .4.1.311.60.2.1 .1、1.3.6.1 .4.1.311.60.2.1 .2、1.3.6.1 .4.1.311.60.2.1 .3。

公钥	根据 RFC 5280 编码，使用 CP 第 7.1.3 中指定的算法，密钥长度满足 CP 第 6.1.5 指定的要求

Table - Basic domain of Certificate structure

domain	Value or value limitation
Version	Format version of X.509 certificate with the value is V3
Serial number	Unique identifier of certificate
Signature algorithm	Signature algorithm for issuing certificate (see CP section 7.1.3)
Issuer DN	Issuer's Distinguish Name
Start period	Based on the Coordinated Universal Time (UTC), Synchronized with Beijing time, encoding follows the requirements of RFC 5280.
End period	Based on the Coordinated Universal Time (UTC), Synchronized with Beijing time, encoding follows the requirements of RFC 5280. The setting of valid period follows the limitation of this CP Section 6.3.2 specified.
Subject DN	Certificate holder or entity DN, including: CN,OU,O,streetAddress,postalCode,L,ST,C,serialNumber,businessCategory, 1.3.6.1.4.1.311.60.2.1.1,1.3.6.1.4.1.311.60.2.1.2,1.3.6.1.4.1.311.60.2.1.3
Public key	Using specified algorithm of CP Section 7.1.3 according to the encode of RFC 5280，key length meets specified requirements of CP Section 6.1.5.

7.1.1. 版本号 Version Number(s)

GDCA 订户的 EV 证书符合 X.509 V3 证书格式，版本信息存放在证书版本信息栏内。

GDCA certificates are in line with X.509 V3 certificate format. The version information is stored in the field of the certificate version column.

7.1.2. 证书扩展项 Certificate Extensions

GDCA 签发的 EV 证书，其证书扩展项遵循 IETF RFC 5280 标准，并符合 Guidelines For The Issuance And Management Of Extended Validation Certificates 的要求。

证书策略扩展应当明确记录在 EV CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 9.3 部分的要求相一致。

Extensions of EV certificate issued by GDCA follow IETF RFC 5280 standard, and conform to the requirements of the Guidelines "for The Issuance and Management of Extended Validation Certificates".

Certificate policy extensions shall be stated definitely in GDCA EV CPS and be accordance with guidelines Section 9.3 released by CA/Browser Forum atwww.cabforum.org.

7.1.3. 算法对象标识符 Algorithm Object Identifiers

GDCA 签发的证书中，密码算法的标识符为 sha256RSA 和 sha256ECDSA。

The cryptographic algorithm identifiers of certificates issued by GDCA include sha1RSA, sha256RSA and sha256ECDSA.

GDCA 所使用的算法对象标识符，符合 ISO 对象标识符（OID）管理的规范。例如：

Algorithm object identifiers used by GDCA are in accordance with ISO object identifier (OID) management standards. For example:

1. 签名算法：

sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {

iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1)

pkcs-1 (1) 5 }

2. 摘要算法：

sha-1 OBJECT IDENTIFIER ::= {

iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26}

md5 OBJECT IDENTIFIER ::={

iso(1) member-body(2) us(840) rsadsi(113549) digestAlgorithm(2) 5}

3. 非对称算法：

rsaEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 1}

4. 对称算法

本 CP 建议使用国家密码管理部门认可的对称算法。

1. Signing Algorithm:

sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {

iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1)

pkcs-1 (1) 5 }

2. Digest Algorithm:

sha-1 OBJECT IDENTIFIER ::= {

iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26}

md5 OBJECT IDENTIFIER ::={

iso(1) member-body(2) us(840) rsadsi(113549) digestAlgorithm(2) 5}

3. Asymmetric Algorithm

rsaEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 1}

4. Symmetric Algorithm

This CP recommends the user to use the symmetric algorithm approved by OSCCA.

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。

EV 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.

EV 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

不适用。

Not applicable.

7.1.6. 证书策略对象标识符 Certificate Policy Object Identifier

GDCA 签发的 EV 证书应包含证书策略的对象标识符，具体可参见本 CP 第 1.4.1.3 节。

证书策略标识符应当明确记录在 EV CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 9.3 部分的要求相一致。

EV certificate issued by GDCA shall contain the certificate policy object identifier: Please refer to CP section1.4.1.3 for details.

Certificate policy object identifier of shall be stated definitely in GDCA EV CPS and be accordance with guidelines Section 9.3 released by CA/Browser Forum atwww.cabforum.org.

7.1.7. 策略限制扩展项的用法 Usage of Policy Constraints Extension

不适用。

Not applicable.

7.1.8. 策略限定符的语法和语义 Policy Qualifiers Syntax and Semantics

不适用。

Not applicable.

7.1.9. 关键证书策略扩展项的处理语义 Processing Semantics for the Critical Certificate Policies Extension

与 X509 和 PKIX 规定一致。

It is in accordance with X509 and PKIX regulations.

7.2. 证书撤销列表 CRL Profile

GDCA 定期签发 CRL，供用户查询使用。

依本 CP 签发的 CRL 符合 RFC3280 标准。CRL 至少包含如下表所述基本域和内容。

The CRL determined in this CP is accordance with RFC5280. CRL contains at least basic domain and content described in the following table:

域	值或者值的限制
版本	V2
颁发者	签发 CRL 的实体，颁发者甄别。
生效日期	CRL 的签发日期
下次更新	CRL 下次签发的日期。最终订户证书每隔 24 小时更新
签名算法	签发 CRL 所使用的签名算法
颁发机构密钥标识符	由 160 位的颁发证书机构公钥进行散列运算后的值构成

撤销列表	列出撤销的证书，包括撤销证书的序列号和撤销日期

Domain	Value or value limitation
Version	V2
Issuer	Entity for issuing CRL, issuer distinguish.
This update	Issuance date of CRL.
Next update	Next issuance date of CRL.CRL is updated every 24 hours.
Signature	signature algorithm used for issuing CRL.
Authority key identifier	It's composed ofa160-bithashofthe value of CA's public key.
Revoked Certificates	List of the revoked certificates, including serial number and revocation date of revocation certificate.

7.2.1. 版本 Version Number(s)

GDCA 目前签发 X.509 V2 版本的 CRL，此版本号存放在 CRL 版本格式栏目中。

GDCA currently issues CRL of X.509 V2 version. This version number is stored in format column of CRL.

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

不适用。

Not applicable.

7.3. OCSP 描述 OCSP Profile

GDCA 为用户提供 OCSP（在线证书状态查询服务），OCSP 作为 CRL 的有效补充，方便证书用户及时查询证书状态信息。

As an effective supplement of CRL, OCSP provided by GDCA is used to check the information of certificate status for subscriber online.

7.3.1. 版本号 Version Number(s)

RFC6960 定义的 OCSP 版本。

The field conforms to OCSP defined in RFC 6960.

7.3.2. OCSP 扩展项 OCSP Extensions

不适用。

Not applicable.

8. 认证机构审计和其他评估 Compliance Audit and Other Assessments

8.1. 评估的频度和情形 Frequency and Circumstances of Assessment

GDCA 应每年对物理控制、密钥管理、操作控制、鉴证执行等情况执行一次审计，以确定实际发生情况是否与预定的标准、要求一致，并根据审查结果采取行动；每季度内部进行一致性审计和运营评估，并每次分别抽取至少 3%数量的 EV SSL 服务器证书和 EV 代码签名证书进行评估，以保证证书服务的可靠性、安全性和可控性。

除了内部审计和评估外，GDCA 还聘请独立的审计师事务所，按照 WebTrust 对 CA 的规则进行外部审计和评估：

1、根据《中华人民共和国电子签名法》、《电子认证服务管理办法》等的的要求，每年一次接受主管部门的评估和检查。

2、GDCA 按照国家主管部门的要求、国家相关标准和本 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。

审计操作应当明确记录在 EV CPS 中，并且要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 17 部分的要求相一致。

GDCA shall audit physical controls, key management, operation controls and authentication once a year in order to confirm the actual circumstance and take actions according to the audit result. Furthermore, GDCA shall make consistency audits and operation assessments quarterly, and GDCA shall extract at least 3% of the EV SSL certificates and EV code signing certificates respectively for assessment to ensure the reliability, security and controllability of certification services.

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.

Audit operation shall be stated definitely in GDCA EV CPS and be accordance with guidelines Section 17 released by CA/Browser Forum at www.cabforum.org.

8.2. 评估者的身份/资格 Identity/Qualifications of Assessor

GDCA 的内部审计，由 GDCA 安全策略委员会负责组织跨部门的审计评估小组，由审计评估小组执行此项工作。

GDCA 聘请的外部审计机构，应该具备以下的资质：

1. 必须是经许可的、有执业资格的评估机构，在业界享有良好的声誉
2. 了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和操作
3. 具备检查系统运行性能的专业技术和工具
4. 具备独立审计的精神

Cross department audit assessment group organized by GDCA Security Policy Committee performs internal audit of GDCA.

External auditors which GDCA hires shall have the following qualifications:

1. Must be an authority which has been licensed and has a good reputation;
2. Understand computer information security system, communication network security requirements, PKI technology, and related standards and operations.
3. Have the expertise and tools to check the system operation and functionality.
4. Be independent.

8.3. 评估者与被评估者之间的关系 Assessor's Relationship to Assessed Entity

1. GDCA 审计员与本机构的系统管理员、业务管理员、业务操作员的工作岗位不能重叠。
2. 外部评估者(信息产业主管部门、独立审计师事务所以及其他机构)和 GDCA 之间是独立的关系，没有任何的业务、财务往来，或者其它任何利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对 GDCA 进行评估。

1. Segregation of duties is required between the GDCA auditors, and the GDCA system administrators, business administrators, and business operators.
2. The external evaluators (information industry department, independent audit firms and other authorities) and GDCA are independent from each other. There are no business interactions, financial transactions, or any other interests that could affect the objectivity of the assessment between the above two. Assessors shall evaluate GDCA in an independent, fair and unbiased attitude.

8.4. 评估的内容 Topics Covered by Assessment

GDCA 内部审计的内容包括：

1. 安全策略是否得到充分的实施；
2. 运营工作流程和制度是否得到严格遵守；
3. 是否严格按 CP、业务规范和安全要求开展认证业务；
4. 各种日志、记录是否完整，是否存在问题；
5. 是否存在其他可能存在的安全风险。

第三方审计师事务所按照 WebTrust For CA 规范的要求，对 GDCA 进行独立审计。

GDCA's internal audit includes:

1. Whether the security strategy is fully implemented

2. Whether operation procedures and processes strictly followed
3. Whether strictly following the CP, business specifications and security requirements when conducting authentication services
4. Whether all kinds of logs and records are preserved and if there is any question
5. If there's any other potential security risks

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

8.5. 对问题与不足采取的行动 Actions Taken as a Result of Deficiency

对于 GDCA 内部审计结果中的问题，由审计评估小组负责监督这些问题的责任职能部门进行业务改进和完善的情况。完成对审计结果的改进后，各职能部门必须向审计评估小组提交业务改进工作总结报告。

对于 GDCA 授权注册机构的审计结果，如该机构正在进行违反本 CP 及 GDCA 制定的其他业务规范的行为，GDCA 将予以制止，并有权责令其立即停止这些行为，同时根据 GDCA 的要求进行业务整改。业务违规行为情节严重的注册机构，GDCA 将终止对该机构的电子认证业务有关授权。

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 CP and other business standards defined by GDCA, GDCA will stop the above behaviors immediately and ask them to make changes in accordance with the requirements of GDCA.GDCA will terminate relevant authorization of electronic certification services of RA if the above behaviors are seriously violated.

If assessments of a third-party auditor firm are completed, GDCA will rectify in accordance with the audit reports. GDCA will be evaluated again after the rectification.

8.6. 评估结果的传达与发布 Communications of Results

GDCA 的内部审计结果应向本机构各职能部门以及审计涉及的注册机构进行正式通报，对可能造成订户安全隐患，GDCA 必须及时向订户通报。

第三方审计师事务所评估完成后，对于审计的结果，将通过 www.gdca.com.cn 网站进行公布。任何第三方向被评估实体通知评估结果或者类似的信息，都必须事先明确向 GDCA 表明通知的目的和方式，并征得 GDCA 的同意，法律另有规定的除外；GDCA 保留在这方面的法律权力。

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 (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

GDCA 可根据提供的电子认证服务向本机构的证书订户收取费用，具体收费标准根据行业市场收费情况而定，GDCA 不得擅自提高收费标准,扩大收费范围。

GDCA can charge the certificate subscriber of this institution for the electronic authentication service. The specific charge standards must be executed according to the market. GDCA can't increase the fees of charge and enlarge the range of charge by itself.

9.1.1. 证书新增和更新费用 Certificate Issuance or Renewal Fees

GDCA 对证书新增和更新的费用，公布在 GDCA 的网站 www.gdca.com.cn 上，供用户查询。

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。

The fees of GDCA adding and renewing certificates are published in the website www.gdca.com for user to query.

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

9.1.2. 证书查询费用 Certificate Access Fees

对于证书查询，目前 GDCA 不收取任何费用。除非用户提出的特殊需求，需要 GDCA 支付额外的费用，GDCA 将与用户协商收取应该收取的费用。

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

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 (www.gdca.com.cn).

9.1.3. 撤销和状态信息查询费用 Revocation or Status Information Access Fees

对于撤销和状态信息查询，目前 GDCA 不收取任何费用。除非用户提出的特殊需求，需要 GDCA 支付额外的费用，GDCA 将与用户协商收取应该收取的费用。

如果撤销和状态信息查询的收费政策有任何变化，GDCA 将会及时在网站 www.gdca.com.cn 上予以公布。

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 (www.gdca.com.cn).

9.1.4. 其他服务费用 Fees for Other Services

1. 如果用户向 GDCA 索取纸质的 CP 或其他相关的作业文件时，GDCA 需要收取因此产生的邮递和处理工本费。
2. GDCA 将向用户提供证书存储介质及相关服务，GDCA 在与订户或者其他实体签署的协议中指明该项价格。
3. 其他 GDCA 将要或者可能提供的服务的费用，GDCA 将会及时公布，供用户

查询。

1. If subscriber requests paper version of CP or other related documents from GDCA, GDCA will charge postage and processing fees.
2. GDCA provides certificate storage media and related services to subscribers. GDCA declares the prices of above items in the agreements signed with subscribers or other entities.
3. Other services fees that GDCA may or will charge will be published timely for referencing.

9.1.5. 退款策略 Refund Policy

GDCA 对订户收取的费用，除了证书申请和更新费用因为特定理由可以退还外，GDCA 均不退还用户任何费用。

在实施证书操作和签发证书的过程中，GDCA 遵守严格的操作程序和策略。如果 GDCA 违背了本 CP 所规定的责任或其它重大义务，订户可以要求 GDCA 撤销证书并退款。在 GDCA 撤销了订户的证书后，GDCA 将立即把订户为申请该证书所支付的费用全额退还给订户。

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 CP or other material obligations, subscribers can request GDCA to revoke certificates and refund. After GDCA revokes subscriber's certificates, GDCA will immediately refund the full amount that subscribers have paid for the certificate application.

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

保险范围主要针对 CP 第 9.9 节中所规定的赔偿。

Insurance Coverage mainly focuses on compensation specified in CP Section 9.9.

9.2.2. 其他财产 other Assets

不适用。

Not applicable.

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

证书订户一旦接受 GDCA 的证书，或者通过协议完成对证书服务的接受，那么就意味着该订户已经接受了本 CP 关于保险和担保的规定和约束。

The acceptance of the certificate or its services specified by the agreement by the subscriber means that subscriber has accepted the specification and constraint of insurance and warranty coverage in this CP.

9.3. 业务信息保密 Confidentiality of Business Information

9.3.1. 保密信息范围 Scope of Confidential Information

在 GDCA 提供的电子认证服务中，以下信息视为保密信息：

1. GDCA 订户的数字签名及解密密钥；
2. 审计记录包括：本地日志、服务器日志、归档日志的信息，这些信息被 GDCA 视为保密信息，只有安全审计员和业务管理员可以查看。除法律要求，不可在公司外部发布；
3. 其他由 GDCA 和 RA 保存的个人和公司信息应视为保密，除法律要求，不可公布。

In the electronic certification service provided by GDCA, the following information is treated as confidential information:

1. GDCA subscriber’s digital signature and decryption key
2. Audit records including local logs, server logs, archive logs information, which is treated by GDCA as confidential information. These records can only be accessed by security auditors and business administrators. Unless for law requirements, this information cannot be released outside of the company
3. Other individual and company information preserved by GDCA and RA and should be treated as confidential. Unless for law requirements, this information cannot be released to the public

9.3.2. 不属于保密的信息 Information Not Within the Scope of Confidential Information

1. 由 GDCA 发行的证书、证书中的公钥；
2. 证书中的订户信息；
3. 证书撤销列表；
4. 证书策略（CP）、电子认证业务规则（CPS）。

1. Certificate issued by GDCA and its public key.
2. Information of subscriber in the certificate.
3. CRL
4. CP and CPS

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

GDCA、注册机构、订户以及与认证业务相关的参与方等，都有义务按照本 CP 的规定，承担相应的保护保密信息的责任，必须通过有效的技术手段和管理程序对其进行保护。

GDCA, RA, subscribers, relevant entities and parties involved in certification business, have the obligations to assume appropriate responsibility of keeping confidential information in accordance with this CP, and must protect it through effective technical means and management process.

当保密信息的所有者出于某种原因，要求 GDCA 公开或披露他所拥有的保密信息时，GDCA 应满足其要求；同时，GDCA 将要求该保密信息的所有者对这种申请进行书面授权，以表示其自身的公开或者披露的意愿。如果这种披露保密信息的行为涉及任何其他方的赔偿义务，GDCA 不应承担任何与此相关的或由于公开保密信息所造成的损失。保密信息的所有者应承担与此相关的或由于公开保密信息引起的所有赔偿责任。

As confidential-information holder requires GDCA to publish or reveal all his/her/its own confidential information due to some causes, GDCA shall satisfy his/her/its requirements; Also, GDCA shall require the holder’s documentary application and authorization to express his/her/its own will of publishing or revealing.
If any other obligation of compensation is involved in the act of revealing confidential information of the user by GDCA, GDCA will not assume any responsibility for damage concerning it or caused by the act of publishing the user's confidential information. The confidential-information holder shall assume compensatory responsibilities related with it or caused by the opening of confidential

information.

当 GDCA 在任何法律、法规、法院以及其他公权力部门通过合法程序的要求下，必须提供本 CP 中规定的保密信息时，GDCA 应按照法律、法规以及法院判决的要求，向执法部门公布相关的保密信息，GDCA 无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

When facing any requirements of laws and regulations or any demands for undergoing legal process of court and other agencies, GDCA must provide confidential information in this CP, and could publish the relevant confidential information to law-enforcing department according to requirements of laws, regulations, legal doctrines or court judgments. Under this circumstance, GDCA shall not assume any responsibility. The reveal shall not be regarded as a breach of confidential requirement and obligations.

9.4. 个人隐私保密 Privacy of Personal Information

9.4.1. 隐私保密计划 Privacy Plan

GDCA 应制定隐私保密计划对订户的个人信息保密。

GDCA should establish the Non-disclosure plan to protect the privacy information of subscriber.

9.4.2. 作为隐私处理的信息 Information Treated as Private

除了证书中已经包括的信息以及证书状态信息外，订户提供的其他基本信息将被视为隐私处理。作为隐私处理的信息包括：

1. 订户的有效证件号码如身份证号码、单位机构代码；
2. 订户的联系电话；
3. 订户的地址；
4. 订户的银行帐号。

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. Information treated as private includes:

1. Subscriber’s valid documents number such as ID number, organization code
2. Subscriber's telephone number
3. Subscriber’s mailing address and living address
4. Subscriber's bank account number

9.4.3. 不被认为隐私的信息 Information Not Deemed Private

订户持有的证书内包括的信息，以及该证书的状态等，是可以公开的，不被视为隐私信息。

All information in a subscriber certificate and the status information of the certificate, etc. is deemed not private, and shall not be regarded as privacy information.

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

GDCA、注册机构有妥善保管与保护本 CP 第 9.4.2 节中规定的订户隐私信息的责任与义务。

GDCA has the responsibility and obligation for proper custody and protection of the certificate applicant personal privacy described in section 9.4.2.

9.4.5. 使用隐私信息的告知与同意 Notice and Consent to Use Private Information

GDCA 在其认证业务范围内使用所获得的任何订户信息，只用于订户身份识别、管理和服务订户的目的。在使用这些信息时，无论是否涉及到隐私，GDCA 都没有告知订户的义务，也无需得到订户的同意。

Any subscriber information GDCA obtaining within the scope of certification business can only be used for identifying, managing and serving subscribers. When using the information, no matter the privacy is involved or not, GDCA has no obligations to notify subscribers, and no need to obtain subscriber’s consent.

GDCA 在任何法律法规或者法院以及公权力部门通过合法程序的要求下，或者信息所有者书面授权的情况下向特定对象披露隐私信息时，也没有告知订户的义务，并且不需得到订户的同意。

Under any requirements of laws and regulations, and demands for undergoing the legal process of other agencies, or under the circumstance where private information holder submits the written authorization to certain object for publishing the information, GDCA has no obligations to notify subscriber, and to obtain the consent from the subscriber.

GDCA、注册机构如果需要将订户隐私信息用于双方约定的用途以外的目的，事前必须告知订户并获得订户同意和授权，而且这种同意和授权要用可归档的方式（如传真、信函等）。

If GDCA and registration authority shall apply user’s private information to other purposes beyond

the functions agreed between two sides, CA and RA shall notify subscriber to obtain his/her/its agreement and authorization, and the agreement and authorization shall be in the form which can be archived (such as fax and business letters etc.).

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

由于法律执行、法律授权的行政执行的需要，GDCA 将订户的隐私信息提供给有关执法机关、行政执行机关是允许的。包括：

1. 政府法律法规的规定并且经相关部门通过合法程序提出申请；
2. 法院以及公权力部门处理因使用证书产生的纠纷时合法的提出申请；
3. 具有合法司法管辖权的仲裁机构的正式申请。

Due to the need of legal execution as well as administrative execution permitted by legal authorization, GDCA shall provide subscriber's private information to relevant law enforcement agency and administrative enforcement authorities. The above behaviors are permitted. It includes:

1. Submit the application following the legal process required by relevant agencies pursuant to the provisions of laws and regulations.
2. The formal application by court and other agencies when dealing with the dispute of using certificate.
3. The formal application by arbitration agency with legal jurisdiction.

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

如果订户要求 GDCA 提供某类特定客户支援服务如资料邮寄时，GDCA 则需要把订户的联系电话和地址等信息提供给第三者如邮寄公司。

If certificate subscriber requires GDCA to provide some particular customer support services such as mailing materials, GDCA needs to send the subscriber's name, mailing address and other related information to a third-party such as mailing company.

9.5. 知识产权 Intellectual Property Rights

1. GDCA 享有并保留对证书以及 GDCA 提供的所有软件的全部知识产权；
2. GDCA 对数字证书系统软件具有所有权、名称权、利益分享权；
3. GDCA 网站上公布的一切信息均为 GDCA 财产，未经 GDCA 书面允许，他人不能转载用于商业行为；

4. GDCA 发行的证书和 CRL 均为受 GDCA 支配的财产；
5. 对外运营管理策略和规范为 GDCA 财产；
6. 用来表示目录中 GDCA 域中的实体的甄别名（以下简称 DN）以及该域中颁发给终端实体的证书，均为 GDCA 的财产。

1. GDCA reserves and remains full intellectual property rights for all the certificates and software offered by GDCA.
2. GDCA holds ownership, the right of name, the right to share the benefits for certificate system software
3. All the information published at GDCA website is GDCA property. Without written permission of GDCA, others cannot repost them for commercial activities.
4. Certificates and CRLs issued by GDCA are both the properties controlled by GDCA.
5. External operation management strategy and specification are GDCA property.
6. The distinguished name (hereinafter referred to as DN) used to express the GDCA domain entity in the directory and the certificate issued to the terminal in the domain entity are the properties of GDCA.

9.6. 陈述与担保 Representations and Warranties

9.6.1. CA 的陈述与担保 CA Representations and Warranties

GDCA 必须做出如下担保：

1. 签发给订户的证书符合本 CP 的所有实质性要求；
2. 保证其私钥得到安全的存放和保护，GDCA 建立和执行的安全机制符合国家相关政策的规定；
3. 将按本 CP 的规定，及时撤销证书；
4. 将向证书订户通报任何已知的，将在本质上影响订户的证书的有效性和可靠性事件；
5. 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）中的域名拥有使用权或控制权；
6. 验证申请者授权了证书的签发以及申请者代表获得了授权，以代表申请者申请证书；
7. 验证证书中所包含的全部信息的准确性（organizationalUnitName 信息除外）；
8. 采取验证措施以减小证书主题“organizationalUnitName”中所包含的信息存在

误导的可能性；

9. 根据 CPS 3.2 的要求验证申请人的身份；
10. 若 GDCA 与订户无关联，则 GDCA 与订户是合法有效且可执行的订户协议双方，该订户协议符合 CA/浏览器论坛发布的 Baseline Requirements 等要求；若 GDCA 与订户为同一实体或有关联，则申请人代表已认可使用条款；
11. 针对所有未过期的证书的当前状态信息（有效或已撤销）建立及维护全天候的（24x7）公开的信息库。

GDCA must make the following warranties:

1. Certificates issued to subscribers by GDCA must be in line with all substantive requirements of this CP;
2. Ensures that its private key shall be stored and protected securely, and GDCA shall establish and implement security mechanism pursuant to the terms of national relevant policies;
3. Revokes certificate timely in accordance with this CP;
4. Informs subscribers any known events, which will fundamentally affect the validity and reliability of the certificate;
5. Verifies that the applicant either had the right to use, or had control of, the Domain Name(s) 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);
6. 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;
7. Verifies the accuracy of all of the information contained in the certificate(with the exception of the organizationalUnitName information);
8. Implements a procedure for reducing the likelihood that the information contained in the certificate's subject: organizationalUnitName attribute would be misleading;
9. Verifies the identity of the applicant according to section 3.2 of this CPS;
10. Subscriber agreement: That, if GDCA and subscribers are not affiliated, the subscriber and GDCA are parties to a legally valid and enforceable subscriber agreement that satisfies the Baseline Requirements and other requirements published by the CA/Browser Forum, or, if GDCA and subscribers are the same entity or are affiliated, the applicant representative acknowledged the terms of use;
11. Maintains a 24 x 7 publicly-accessible repository with current information regarding the status (valid or revoked) of all unexpired certificates.

GDCA 对依赖方必须做出如下担保：

1. 除未经验证的订户信息外，证书中的其他订户信息都是准确的；

2. GDCA 完全遵照本 CP 及 CPS 的规定签发证书；
3. 在 GDCA 信息库中发布的证书已经签发给了订户，并且订户已经按照本 CP 中的规定接受了该证书。

GDCA must make the following warranties to relying party:

1. GDCA guarantees that the subscriber information in the certificate is accurate except the unauthenticated subscriber information;
2. GDCA is in full compliance with the provisions of the CP and relevant CPS to issue certificate;
3. Certificates published in GDCA repositories should have be issued to subscribers and accepted by subscribers in accordance with the provisions of the CP.

ROOT CA 和 CA 的保证和责任应当明确记录在 EV CPS 中，并且分别要和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 18 和 7.1 部分的要求相一致。

The guarantee and liability of ROOT CA and CA shall be stated definitely in GDCA EV CPS and be in accordance with guidelines Section 18 and 7.1 released by CA/Browser Forum at www.cabforum.org.

9.6.2. RA 的陈述与担保 RA Representations and Warranties

1. 提供给证书订户的注册过程完全符合本 CP 的所有实质性要求；
2. 在 GDCA 生成证书时，不会因为注册机构的失误而导致证书中的信息与证书申请者的信息不一致；
3. 注册机构将按本 CP 的规定，及时向 GDCA 提交证书申请、撤销、更新等服务申请。

1. The registration process provided for subscribers is compliant with all the substantive requirements of GDCA's CP;
2. When generating certificates, GDCA does not allow the inconsistencies between certificate information and certificate applicant information due to mistakes of registration authority;
3. Registration authority will submit the applications of revocation, update and other services to GDCA in time according to the provisions of CP.

9.6.3. 订户的陈述与担保 Subscriber Representations and Warranties

订户一旦接受 GDCA 签发的证书，就被视为向 GDCA、注册机构及依赖方作出以下承诺：

1. 在证书的有效期内进行数字签名；
2. 订户在申请证书时向注册机构提供的信息都是真实、完整和准确的，愿意承担任何提供虚假、伪造等信息的法律责任；
3. 如果存在代理人，那么订户和代理人两者负有连带责任。订户有责任就代理人所作的任何不实陈述与遗漏，通知 GDCA 或其授权的证书服务机构；
4. 与订户证书所含公钥相对应的私钥所进行的每一次签名，都是订户自己的签名，并且在进行签名时，证书是有效证书（证书没有过期、撤销），证书的私钥为订户本身访问和使用；
5. 除非经订户和发证机构间书面协议明确规定，订户保证不从事发证机构（或类似机构）所从事的业务；
6. 一经接受证书，即表示订户知悉和接受本 CP 中的所有条款和条件，并知悉和接受相应的订户协议；
7. 一经接受证书，订户就应当承当如下责任：始终保持对其私钥的控制，使用可信的系统，采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用；
8. 不得拒绝任何来自 GDCA 公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等；
9. 证书在本 CP 中规定使用范围内合法使用，只将证书用于经过授权的或其他合法的使用目的；
10. 采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件；
11. 对于 EV SSL 证书，订户有责任和义务保证只在证书中列出的主题别名对应的服务器中部署证书；
12. 对于 EV 代码签名证书，订户不得将其用于可疑代码等非法软件、恶意软件的签名。

Once subscribers accept a certificate issued by GDCA, the subscriber is considered to make the following commitments to GDCA, registration authority and related parties who trust the certificate:

1. The subscriber uses digital signatures if the certificate is valid;
2. All information that subscriber provides to registration authority during certificate application process must be true, complete and accurate. The subscriber is willing to take legal responsibility for any false or forged information;
3. If there is an agent, then both the subscriber and agent take jointly responsibility. The subscriber is responsible for notifying GDCA and its authorized certification services agencies any false statements and omissions made by the agent;

4. Each signature is generated using the private key corresponding to certificate by subscribers themselves. The certificates shall be valid at the moment of signing, i.e. certificate is not revoked or expired;

5. Subscribers ensure that they don't engage in business performed by the issuing agency (or similar institutions) unless they sign written agreements with the issuing agency on such matters;

6. Once the certificate is accepted, subscribers are considered as knowing and accepting all the terms and conditions in the CP as well as corresponding subscriber agreements;

7. Once the certificate is accepted, the subscriber should assume the following responsibilities: always maintain control of their private keys; use trustworthy systems; and take reasonable precautions to prevent the loss, disclosure, alteration, or unauthorized usage of the private keys;

8. Prohibited for rejecting any statements, changes, updates and upgrades published by GDCA, including but not limited to modification of strategies and standards as well as additions and deletions of certificate services;

9. The subscriber only uses certificate for the authorized or other lawful purpose within the range specified by this CP;

10. The subscriber use secure and reasonable measures to prevent the private key from loss, disclosure, alteration and other events;

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

12. The subscriber must not use the EV code signing certificates for signing suspicious codes and other illegal or malicious software.

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

1. 遵守本 CP 的所有规定；
2. 在依赖证书前，确认证书在规定的范围和期限使用；
3. 在依赖证书前，对证书的信任链进行验证；
4. 在依赖证书前，通过查询 CRL 或 OCSP 确认证书是否被撤销；
5. 一旦由于疏忽或者其他原因违背了合理检查的条款，依赖方愿意就此而给 GDCA 带来的损失进行补偿，并且承担因此造成的自身或他人的损失；
6. 不得拒绝任何来自 GDCA 公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

1. Abide by all provisions of this CP.

2. Ensure that the certificate is used in prescribed scope and duration;

3. Verify certificate's trust chain before trust the certificate;
4. Before trust a certificate, verify whether the certificate is revoked or not through querying CRL or OCSP;
5. The relying party is willing to compensate GDCA for the losses and accept liabilities for any loss of self or others, due to negligence or other reasons violating the terms of a reasonable inspection;
6. Prohibited for rejecting any statements, changes, updates and upgrades published by GDCA, including but not limited to modification of strategies and standards as well as additions and deletions of certificate services.

9.6.5. 其他参与者的陈述与担保 Representations and Warranties of Other Participants

遵守本 CP 的所有规定。

Abide by all provisions of this CP.

9.7. 担保免责 Disclaimers of Warranties

除本 CP 9.6.1 中的明确承诺外，GDCA 不承担其他任何形式的保证和义务：

1. 不保证证书订户、依赖方、其他参与者的陈述内容；
2. 不对电子认证活动中使用的任何软件做出保证；
3. 不对证书在超出规定目的以外的应用承担任何责任；
4. 对由于不可抗力，如战争、自然灾害等造成的服务中断并由此造成的客户损失承担责任；
5. 订户违反本 CP9.6.3 之承诺时，或依赖方违反本 CP9.6.4 之承诺时，得以免除 GDCA 之责任。

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

1. Do not guarantee the statements of certificate subscribers, relying party and other;
2. Do not guarantee any software used in electronic certification activities;
3. Do not assume any liability when certificate is used beyond the prescribed purposes;
4. Do not assume any responsibility for service interruption and customer losses caused by force majeure, such as war, natural disasters, etc;
5. When subscriber violates the commitments defined in CP Section 9.6.3, or relying party

violates the commitments defined in CP Section 9.6.4, GDCA can exempt from liability.

9.8. 有限责任 Limitations of Liability

证书订户、依赖方因 GDCA 提供的电子认证服务从事民事活动遭受损失，GDCA 只承担本 CP9.9.1 规定的有限责任。

The certificate subscriber and the relying party specialized in civil activities suffered losses due to electronic certification service provided by GDCA, GDCA only assume limited liability amount stipulated in CP section 9.9.1.

9.9. 赔偿 Indemnities

9.9.1. 认证机构的赔偿责任 Indemnification by GDCA

如 GDCA 违反了本 CP 第 9.6.1 节中的陈述，订户、依赖方等实体可申请 GDCA 承担赔偿责任（法定或约定免责除外），包括以下情形：

1. GDCA 将证书错误的签发给订户以外的第三方，导致订户或依赖方遭受损失的；
2. 在订户提交信息或资料准确、属实的情况下，GDCA 签发的证书出现了错误信息，导致订户或依赖方遭受损失的；
3. 在 GDCA 明知订户提交信息或资料存在虚假谎报的情况，但仍然向订户签发证书，导致依赖方遭受损失的；
4. 由于 GDCA 的原因导致 CA 私钥的泄露；
5. GDCA 未能及时撤销证书，导致依赖方遭受损失的。

If GDCA violates statements in CP Section 9.6.1, certificate subscribers, relying parties and other entities can request GDCA assume compensation liabilities (except for statutory and contractual exemptions). If the following circumstances occur, GDCA will assume limited compensation liability:

1. GDCA issues certificates to a third-party instead of the subscriber by mistake, which leads to losses of the subscriber or relying party.
2. If subscriber submits accurate and true information to GDCA, but GDCA issues certificates with error information and the error leads to losses of the subscriber or relying party.
3. After GDCA knows the fact that subscriber provides fake registration information or data, GDCA still issues certificate, which leads to relying party suffering losses.
4. If the private key of CA is disclosed due to GDCA's fault.
5. GDCA fails to revoke certificates in time, which leads to relying party suffering losses.

9.9.2. 订户的赔偿责任 Indemnification by Subscribers

在如下情况，订户对自身原因造成的 GDCA、依赖方损失，应当承担赔偿责任：

1. 订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致 GDCA 及其授权的证书服务机构或者第三方遭受损害；
2. 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知 GDCA 及其授权的证书服务机构，以及不当交付他人使用造成 GDCA 及其授权的证书服务机构、第三方遭受损害；
3. 订户使用证书的行为，有违反本 CP 及相关操作规范，或者将证书用于非本 CP 规定的业务范围；
4. 证书订户或者其它有权提出撤销证书的实体提出撤销请求后，到 GDCA 将该证书撤销信息予以发布的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果 GDCA 按照本 CP 的规范进行了有关操作，那么该证书订户必须承担所有损害赔偿责任；
5. 证书中的信息发生变更但未停止使用证书并及时通知 GDCA 和依赖方；
6. 没有对私钥采取有效的保护措施，导致私钥丢失或被损害、窃取、泄露等；
7. 在得知私钥丢失或存在危险时，未停止使用证书并及时通知 GDCA 和依赖方；
8. 证书到期但仍在使用证书；
9. 订户的证书信息侵犯了第三方的知识产权；
10. 在规定的应用范围外使用证书，如从事违法犯罪活动。

If the following situations cause GDCA or relying party suffering losses, subscribers shall be assumed the liability to compensate:

1. GDCA and its authorized service agencies or third-party suffer losses due to unreal information, such as deliberate, negligent or malicious provision of unreal information by applicants when applying for certificates.
2. GDCA and its authorized service agencies or third-party suffer losses due to disclosure and loss of private keys deliberately and by mistake; due to not informing GDCA and its authorized service agencies or third-party of the leakage and loss of private keys with knowing the facts; and due to handing keys to others inappropriately.
3. Subscribers violate the CP and related operation practices when using certificates as well as using the certificates activities outside of the CP.
4. If the certificate is used for illegal transactions or causes disputes during the period from revocation requests submitted by the subscribers or other entities authorized by GDCA to this information of certificate revocation published by GDCA, if GDCA operates in accordance with

the requirements of the CP, subscribers must assume any responsibility of losses according to this CP.

5. Subscribers do not stop to use the certificate which its information have changed and don't notify it to GDCA or relying parties in time.
6. The private key is lost, compromised, stolen, exposed, and etc. due to not taking effective protection measures.
7. Subscribers do not stop to use the certificate which its private key is lost or in danger and notify it to GDCA or relying parties in time.
8. The certificate has expired but is still in use.
9. The subscriber's certificate information infringes upon the intellectual property rights of a third-party.
10. Using certificates outside the provisions of specific application scope, such as the use of certificates for illegal and criminal activities.

9.9.3. 依赖方的赔偿责任 Indemnification by Relying Parties

在如下情况，依赖方对自身原因造成的 GDCA、订户损失，应当承担赔偿责任：

1. 没有履行 GDCA 与依赖方的协议和本 CP 中规定的义务；
2. 未能依照本 CP 规范进行合理审核，导致 GDCA 及其授权的证书服务机构或第三方遭受损害；
3. 在不合理的情形下依赖证书，如依赖方明知证书存在超范围、超期限使用的情形或证书已经或有可能被人窃取的情形，但仍然依赖证书；
4. 依赖方没有对证书的信任链进行验证；
5. 依赖方没有通过查询 CRL 或 OCSP 确认证书是否被撤销。

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

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

9.10. 有效期与终止 Term and Termination

9.10.1. 有效期 Term

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

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

9.10.2. 终止 Termination

GDCA 终止电子认证服务时，本 CP 终止。

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

9.10.3. 终止的效果与存续 Effect of Termination and Survival

本 CP 的终止，意味着认证机构认证业务的终止，但认证业务的终止不意味着认证机构责任的终止。认证机构在业务终止后应采取合理的措施，将认证服务转到其他认证机构，保证订户的利益。

The termination of this CP means that the termination of certification authority business, but the termination of certification business does not mean the termination of certification authority responsibility. After the termination of business, certification authority shall take reasonable measures to transfer certification service to other certification authority so as to ensure the interests of the subscriber.

9.11. 对参与者的个别通告及信息交互 Individual Notices and Communications with Participants

认证机构在必要的情况下，如主动撤销订户证书、发现订户将证书用于规定外用途及订户其他违反订户协议的行为，可通过适当方式，如电话、电子邮件、信函等，个别通知订户、依赖方。

The circumstances that CA actively revokes the subscriber's certificate, finds out subscriber using certificate out of specified usage, or behaviors of subscriber violating subscriber agreement have occurred, CA can use appropriate way, such as telephone, E-mail, letter, Fax, etc., to notify

subscriber and relying party if necessary.

9.12. 修订 Amendments

9.12.1. 修订程序 Procedure for Amendment

经 GDCA 安全策略委员会授权，GDCA 行政管理部每年至少审查一次本 CP，确保其符合国家法律法规和主管部门的要求及最新版本的 SSL 基准要求规范，符合认证业务开展的实际需要。

本 CP 的修订，由 GDCA 行政管理部提出修订报告，获得 GDCA 安全策略委员会批准后，由 GDCA 行政管理部负责组织修订，修订后的 CP 经过 GDCA 安全策略委员会批准后正式对外发布。

Through the authorization of GDCA Security Policy Committee, GDCA Administration and Management Department shall review this CP at least once a year, to ensure that CP meets the requirements of national laws and regulations and administration department, to meet the latest SSL baseline requirements and specifications, and satisfy the actual requirements of certification business operation.

The revised version of this CP will be revised by GDCA Administration Department and approved by GDCA Security Policy Committee. GDCA Administration Department will be responsible for the revision and the revised CP will be officially released after being approved by GDCA Security Policy Committee.

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

修订后的 CP 经批准后将立即在 GDCA 的网站 www.gdca.com.cn 上发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，GDCA 将在合理的时间内通知有关各方，合理的时间应保证有关方受到的影响最小。

After approval of the revised CP, it will be posted on GDCA official website www.gdca.com.cn immediately. For the modification notified by email, mail, media and other ways, GDCA shall notify the relevant parties in reasonable time, which ensures that the relevant parties have minimum influence.

9.12.3. 必须修订的情形 Circumstances Under Which CP Must be Changed

如果出现下列情况，GDCA 必须对本 CP 进行修改：

1. 密码技术出现重大发展，足以影响现有 CP 的有效性；

2. 有关认证业务的相关标准进行更新；
3. 认证系统和有关管理规范发生重大升级或改变；
4. 法律法规和主管部门要求；
5. 现有 CP 出现重要缺陷。

If the following situations occur, this CP must be modified:

1. The encryption technology develops significantly enough to affect the effectiveness of existing CP.
2. The relevant standards have been updated.
3. Certification system and relevant management regulations take significant upgrade or changes.
4. The laws and the administration departments require the CP to be modified.
5. There is some significant deficiency in the existing CP.

9.12.4. 对象标识符变更 Object Identifier Modification

当本 CP 发生修订时，相对应的证书策略对象标识符不会进行变更，仅增加版本识别代码。

When the CP has modified, its corresponding certificate policy object identifier will not change, and only increase the version identification code.

9.13. 争议解决条款 Dispute Resolution Provisions

当 GDCA、订户和依赖方之间出现争议时，有关方面应依据协议通过协商解决，协商解决不了的，可通过法律解决。

Any disputes between GDCA and subscribers or relying parties shall be resolved through negotiations as agreed, and those cannot be settled by negotiations will be resolved by laws.

9.14. 管辖法律 Governing Law

GDCA 的 CP 受国家已颁布的《中国人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》法律法规管辖。

The CP of GDCA is governed by the law of " Electronic Signatures Laws of People's Republic of China", the regulation of "Measures for the Administration of Electronic Certification Services"

and ”Measures for the Administration of Cipher Codes for Electronic Certification Services” promulgated by the country.

9.15. 符合适用法律 Compliance with Applicable Law

认证机构的所有业务、活动、合同、协议必须符合《中国人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》以及其它中华人民共和国法律法规的规定。

All businesses, activities, contacts, agreements of GDCA must conform to "Electronic Signatures Laws of People’s Republic of China”, “Measures for the Administration of Electronic Certification Services”, “Measures for the Administration of Cipher Codes for Electronic Certification Services” and other laws and regulations of People’s Republic of China.

9.16. 一般条款 Miscellaneous Provisions

9.16.1. 完整协议 Entire Agreement

CP、CPS、订户协议、依赖方协议及其补充协议将构成 PKI 参入者之间的完整协议。

The entire agreement is composed of CP, CPS, Subscriber Agreement and Relying Party Agreement as well as its supplementary agreement.

9.16.2. 让渡 Assignment

根据本 CP 中详述的认证实体各方的权利和义务，各方当事人可按照法律的相关规定进行权利和义务的转让。此转让行为发生时不影响到转让方对另一方的任何债务及责任的更新。

According to the rights and obligations of certification entity parties detailed in this CP, all parties can transfer the possession of rights and obligations in accordance with the relevant provisions of the law. The occurrence of the above transfer behavior does not affect the change of any debt and liability among the transferors.

9.16.3. 分割性 Severability

如果本 CP 的任何条款或其应用由于与 GDCA 所在管辖区的法律产生冲突而被判定为无效或不具执行力时，GDCA 应在最低必要的限度下修订该条款，使其继续有效，其余部分不受影响，GDCA 应在此章节批露修订的内容。

在根据修订后要求签发证书之前，GDCA 应发送邮件至 question@cabforum.org，通知 CAB 论坛 CP 中已修订的信息，并确认其已被发至公共邮件列表和存在于公共档案列表(https://cabforum.org/pipermail/public/)。

若法律不再适用，或 CA/B 论坛的要求被修改，使 GDCA 同时符合 CA/B 论坛的 Baseline Requirements 及法律要求，则本章节中任何对 GDCA 业务操作的调整应不再继续适用。上述对业务操作进行的相关调整，对 GDCA 的 CP 的修订，及向 CA/B 论坛的通知应在 90 天内完成。

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

GDCA shall (and prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of any modified content in the CP by sending emails to question@cabforum.org, and confirm that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/.

Any modification to GDCA's practice enabled under this section shall be discontinued if and when the law no longer applies, or the requirements published by the CA/B Forum are modified to make it possible to comply with both them and the law simultaneously. An appropriate change in practice, modification to the GDCA's CP and a notice to the CA/Browser Forum, as outlined above, shall be made within 90 days.

9.16.4. 强制执行 Enforcement

不适用。

Not applicable.

9.16.5. 不可抗力 Force Majeure

依据本 CP 制定的 CPS 应包括不可抗力条款，以保护各方利益。

CPS formulated in accordance with this CP shall include a force majeure clause to defend the benefits of each party.

9.17. 其他条款 Other Provisions

GDCA 对本 CP 具有最终解释权。

GDCA has final interpretation rights to this CP.

附录：GDCA EV 证书策略修订记录表

Appendix: GDCA EV CP Revision Records

内容 / 序号	修订章节	V1.9	V2.0
1	6.3.2.证书操作期和密钥对使用期限 Certificate Operational Periods and Key Pair Usage Periods		将 SSL/TLS 服务器证书密钥对的最长允许使用期限调整为 398 天。
2	其他修订		修订一些语法及文字上容易引起歧义的地方。

Content / SEQ	Sections Revised	V1.9	V2.0
1	6.3.2.证书操作期和密钥对使用期限 Certificate Operational Periods and Key Pair Usage Periods		Adjusted the maximum usage period of the key pair for SSL/TLS certificates to 398 days.
2	Other revisions		Adjusted some wording issues, and other parts that may cause confusion.