贵州省电子认证科技有限公司

证书策略

（CP）

版本：V1.0

发布日期：2023 年 5 月 5 日

生效日期：2023 年 5 月 5 日

地址：中国贵州省贵阳市长岭南路178号 邮编：550081
电话：+86-851-85559301 传真：+86-851-85559784
网址：https://www.gzca.cn

版 本 控 制 表

版本	AMD	修订说明	修订人	审核人/批准人	发布&生效日期
V1.0	A		田勇	GZCA 安委会	2023 年 5 月 5 日

（A-添加，M-修改，D-删除）

地址：中国贵州省贵阳市长岭南路178号 邮编：550081
电话：+86-851-85559301 传真：+86-851-85559784
网址：https://www.gzca.cn

目 录

1. 引言

1.1. 概述

1.1.1. 公司简介

贵州省电子认证科技有限公司（GuiZhou Electronic Certificate CO.,LTD.简称 GZCA），成立于 2005 年 6 月，具备电子认证服务使用密码资质（证书编号：0039），是国家工信部批准的“电子认证服务机构”（许可证编号：ECP52010314037）、国家密码管理局批准的“电子政务电子认证服务机构”（编号：A033），是贵州省网络信任体系的重要组成部分。

GZCA 是严格按照《中华人民共和国电子签名法》、《电子认证服务管理办法》的要求来设立，为订户和依赖方提供数字证书申请、签发、更新、查询、注销等服务，并以 PKI 技术、数字证书应用技术为电子政务、电子商务、企业信息化构建安全、可靠的信任环境。

GZCA 本着“诚信、保密、满意”的服务宗旨，致力于电子认证服务。

1.1.2. 证书策略(CP)

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

本 CP 满足《互联网 X.509 公开密钥基础设施证书策略和证书业务框架》（Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework），即由互联网标准组织“互联网工程工作组”（Internet Engineering Task Force）制定的 RFC3647 标准的结构和内容要求，同时也满足《GB 26855-2011-T 信息安全技术公钥基础设施证书策略

与认证业务声明框架》的结构和内容要求，并根据中国的法律法规和 GZCA 的运营要求进行适当的改变。

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

1.1.3. GZCA 架构

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

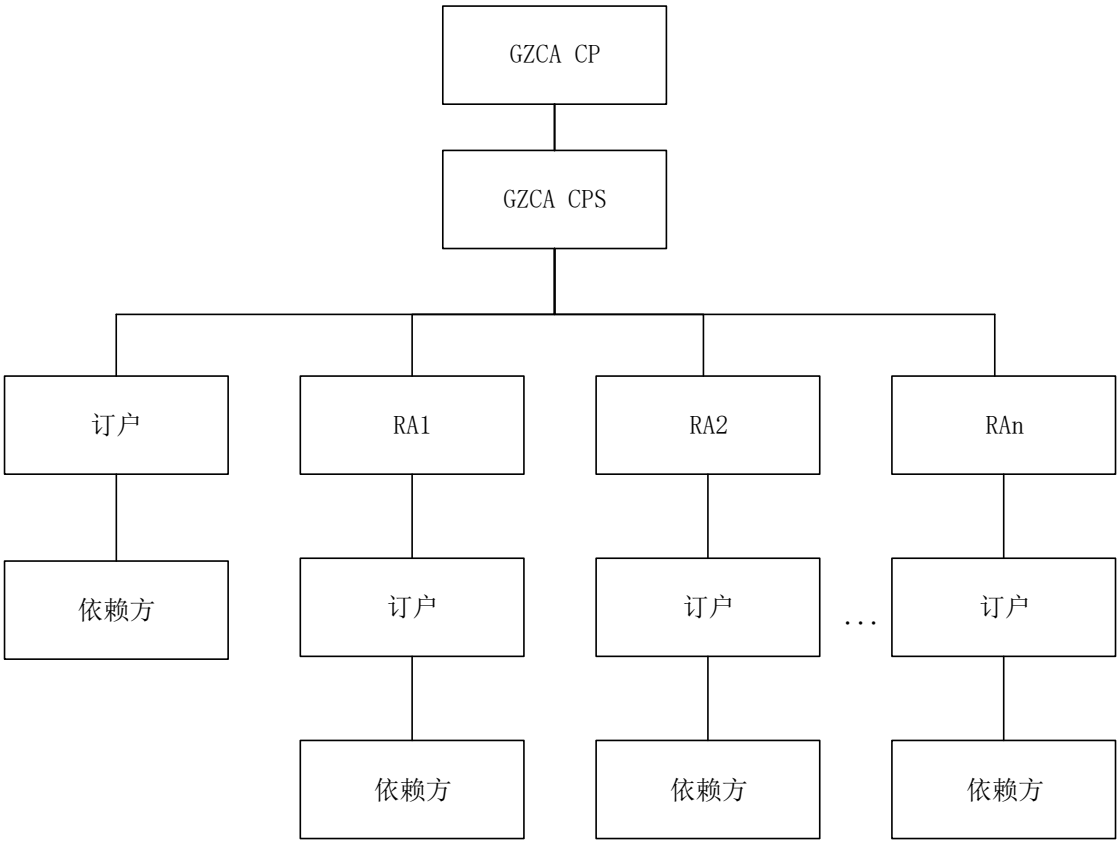

图 1-1 GZCA 架构

1.1.4. GZCA 证书层次架构

GZCA 目前有 3 个根证书，分别为为 ROOTCA 证书（SM2），Guizhou SM2 CA 证书（SM2），Guizhou Root CA 证书（RSA）。每个根 CA 下设中级 CA，以签发用户证书。除 SSL 证书外，GZCA 不签发外部中级 CA 证书。

1) ROOTCA (SM2)

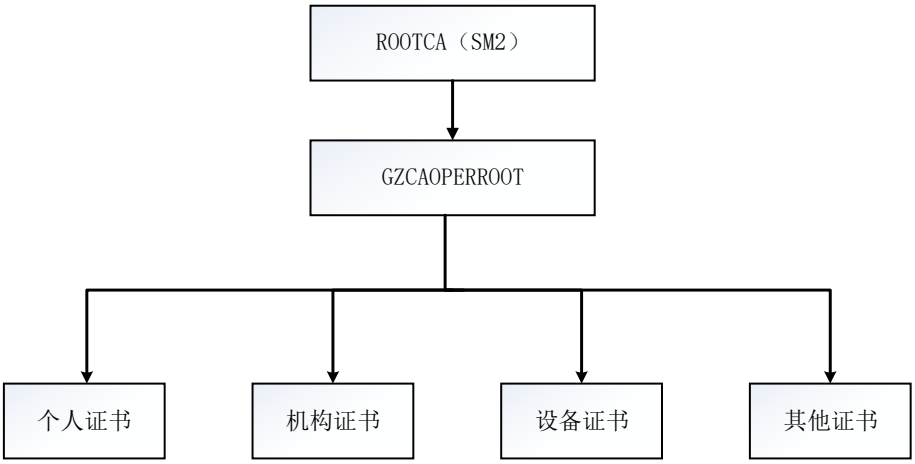

图 1-2 GZCAOPERROOT 证书架构

ROOTCA 证书（SM2）是国家密码管理局的根证书，密码算法为 SM2，根密钥长度为256-bit,下设 GZCAOPERROOT 证书,密钥长度为256-bit,签发算法为 SM2，密钥长度为 256-bit 的 个人类证书、机构类证书、设备类证书和其他类证书。

ROOTCA 证书（SM2）将于 2042 年 7 月 7 日到期。

GZCAOPERROOT 证书将在 2034 年 2 月 8 日到期，2023 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

2) ROOTCA (SM2)

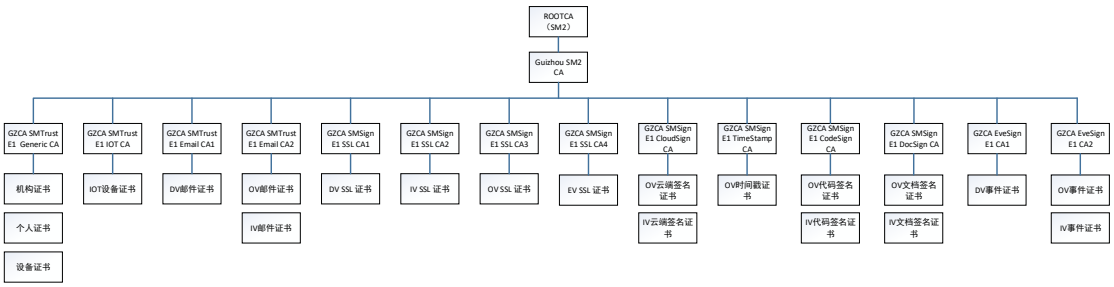

图 1-2 GZCA SM2 CA 证书架构

ROOTCA 证书（SM2）是国家密码管理局的根证书，密码算法为 SM2，根密钥长度为256-bit；下设 Guizhou SM2 CA 根证书，密钥长度为256-bit；下设 GZCA SMTrust E1 Generic CA 业务根证书，密钥长度为256-bit，签发算法为 SM2，密钥长度为 256-bit 的 个人证书、机构证书、设备证书；下设 GZCA SMTrust E1 IOT CA 业务根证书,密钥长度为256-bit,签发算法为 SM2,密钥长度为 256-bit 的 IOT 设备证书；下设 GZCA SMTrust E1 Email CA1 业务根证书，密钥长度为256-bit，签发算法为 SM2，密钥长度为 256-bit 的 DV 邮件证书；下设 GZCA SMTrust E1 Email CA2 业务根证书，密钥长度为256-bit，签发算法为 SM2，密钥长度为 256-bit 的IV 邮件证书、OV 邮件证书；下设 GZCA SMSign E1 SSL CA1 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 DV SSL 证书；下设 GZCA SMSign E1 SSL CA2 业务根证书，密钥长度为256-bit，签发算法为 SM2,密钥长度为 256-bit 的IV SSL 证书;下设 GZCA SMSign E1 SSL CA3 业务根证书,密钥长度为256-bit,签发算法为 SM2,密钥长度为 256-bit 的 OV SSL 证书；下设 GZCA SMSign E1 SSL CA4 业务根证书，密钥长度为256-bit，签发算法为 SM2，密钥长度为 256-bit 的 EV SSL 证书；下设 GZCA SMSign E1 CloudSign CA 业务根证书，密钥长度为256-bit，签发算法为 SM2，密钥长度为

256-bit 的 IV 云端签名证书、OV 云端签名证书；下设 GZCA SMSign E1 TimeStamp CA 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 OV 时间戳证书；下设 GZCA SMSign E1 CodeSign CA 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 IV 代码签名证书、OV 代码签名证书；下设 GZCA SMSign E1 DocSign CA 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 IV 文档签名证书、OV 文档签名证书；下设 GZCA EveSign E1 CA1 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 DV 事件证书；下设 GZCA EveSign E1 CA2 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 IV 事件证书、OV 事件证书。

ROOTCA 证书（SM2）将于 2042 年 7 月 7 日到期。

Guizhou SM2 CA 证书将在 2042 年 4 月 30 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发下级 CA 证书。

GZCA SMTrust E1 Generic CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMTrust E1 IOT CA 证书将在 2041 年 12 月 31 日到期，2040 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMTrust E1 Email CA1 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMTrust E1 Email CA2 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 SSL CA1 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 SSL CA2 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 SSL CA3 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 SSL CA4 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 CloudSign CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 TimeStamp CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 CodeSign CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 DocSign CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA EveSign E1 CA1 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA EveSign E1 CA2 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

3) Guizhou SM2 CA (SM2)

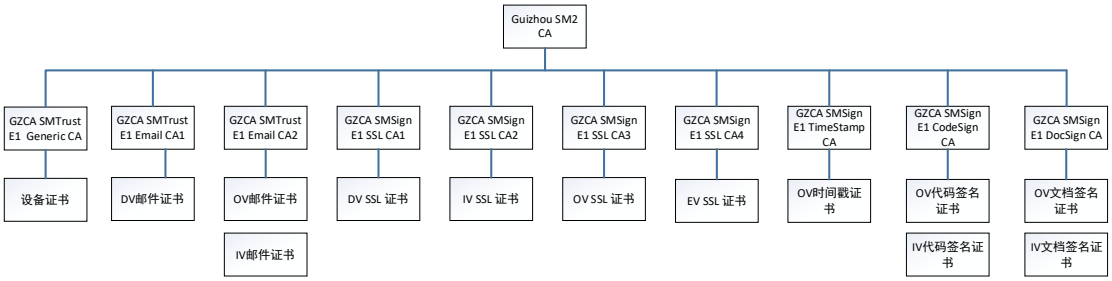

图 1-3 Guizhou SM2 CA 证书架构

Guizhou SM2 CA 证书（SM2）是 GZCA 自签发的根证书，密码算法为 SM2，根密钥长度为 256-bit；下设 GZCA SMTrust E1 Generic CA 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的设备证书；下设 GZCA SMTrust E1 Email CA1 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 DV 邮件证书；下设 GZCA SMTrust E1 Email CA2 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 IV 邮件证书、OV 邮件证书；下设 GZCA SMSign E1 SSL CA1 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 DV SSL 证书；下设 GZCA SMSign E1 SSL CA2 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 IV SSL 证书；下设 GZCA SMSign E1 SSL CA3 业务根证书，密钥长度为 256-bit，

签发算法为 SM2，密钥长度为 256-bit 的 OV SSL 证书；下设 GZCA SMSign E1 SSL CA4 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 EV SSL 证书；下设 GZCA SMSign E1 CloudSign CA 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 IV 云端签名证书、OV 云端签名证书；下设 GZCA SMSign E1 TimeStamp CA 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 OV 时间戳证书；下设 GZCA SMSign E1 CodeSign CA 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 IV 代码签名证书、OV 代码签名证书；下设 GZCA SMSign E1 DocSign CA 业务根证书，密钥长度为 256-bit，签发算法为 SM2，密钥长度为 256-bit 的 IV 文档签名证书、OV 文档签名证书。

Guizhou SM2 CA 证书将在 2042 年 4 月 30 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发下级 CA 证书。

GZCA SMTrust E1 Generic CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMTrust E1 Email CA1 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMTrust E1 Email CA2 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 SSL CA1 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 SSL CA2 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 SSL CA3 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 SSL CA4 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 CloudSign CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 TimeStamp CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 CodeSign CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign E1 DocSign CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

4) Guizhou Root CA（RSA）

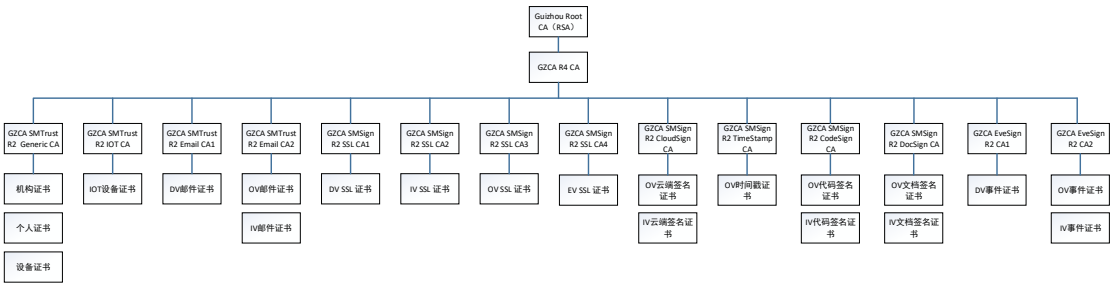

图 1-4 Guizhou Root CA（RSA）证书架构

Guizhou Root CA 证书（RSA）是 GZCA 的根证书，密码算法为 RSA，根密钥长度为 4096-bit；下设 GZCA R4 CA 根证书，密钥长度为 4096-bit；下设 GZCA SMTrust R2 Generic CA 业务根证书，密钥长度为 2048-bit，签发算法为 RSA，密钥长度为 2048-bit 的 个人证书、机构证书、设备证书；下设 GZCA SMTrust R2 IOT CA 业务根证书，密钥长度为 2048-bit，签发算法为 RSA，密钥长度为 2048-bit 的 IOT 设备证书；下设 GZCA SMTrust R2 Email CA1 业务根证书，密钥长度为 2048-bit，签发算法为 RSA，密钥长度为 2048-bit 的 DV 邮件证书；下设 GZCA SMTrust R2 Email CA2 业务根证书，密钥长度为 2048-bit，签发算法为 RSA,密钥长度为 2048-bit 的 IV 邮件证书、OV 邮件证书；下设 GZCA SMSign R2 SSL CA1 业务根证书，密钥长度为 2048-bit，签发算法为 RSA，密钥长度为 2048-bit 的 DV SSL 证书；下设 GZCA SMSign R2 SSL CA2 业务根证书，密钥长度为 2048-bit，签发算法为 RSA，密钥长度为 2048-bit 的 IV SSL 证书；下设 GZCA SMSign R2 SSL CA3 业务根证书，密钥长度为 2048-bit，签发算法为 RSA，密钥长度为 2048-bit 的 OV SSL 证书；下设 GZCA SMSign R2 SSL CA4 业务根证书，密钥长度为 2048-bit，签发算法为 RSA，密钥长度为 2048-bit 的 EV SSL 证书；下设 GZCA SMSign R2 CloudSign CA 业务根证书，密钥长度为 2048-bit，

签发算法为 RSA,密钥长度为 2048-bit 的 IV 云端签名证书、OV 云端签名证书；下设 GZCA SMSign R2 TimeStamp CA 业务根证书，密钥长度为 2048-bit，签发算法为 RSA，密钥长度为 2048-bit 的 OV 时间戳证书；下设 GZCA SMSign R2 CodeSign CA 业务根证书，密钥长度为 2048-bit，签发算法为 RSA，密钥长度为 2048-bit 的 IV 代码签名证书、OV 代码签名证书；下设 GZCA SMSign R2 DocSign CA 业务根证书，密钥长度为 2048-bit，签发算法为 RSA，密钥长度为 2048-bit 的 IV 文档签名证书、OV 文档签名证书；下设 GZCA EveSign R2 CA1 业务根证书，密钥长度为 2048-bit,签发算法为 RSA,密钥长度为 2048-bit 的 DV 事件证书；下设 GZCA EveSign R2 CA2 业务根证书，密钥长度为 2048-bit，签发算法为 RSA，密钥长度为 2048-bit 的 IV 事件证书、OV 事件证书。

Guizhou Root CA 证书（RSA）将于 2052 年 4 月 30 日到期。

GZCA R4 CA 证书将在 2042 年 4 月 30 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发下级 CA 证书。

GZCA SMTrust R2 Generic CA 证书将在 2041 年 12 月 31 日到期，2040 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMTrust R2 IOT CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMTrust R2 Email CA1 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMTrust R2 Email CA2 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign R2 SSL CA1 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign R2 SSL CA2 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign R2 SSL CA3 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign R2 SSL CA4 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign R2 CloudSign CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign R2 TimeStamp CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign R2 CodeSign CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA SMSign R2 DocSign CA 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA EveSign R2 CA1 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

GZCA EveSign R2 CA2 证书将在 2041 年 12 月 31 日到期，2039 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

依据 IETF PKIX RFC 3647 CP/CPS 框架，本 CP 共分为九个章节，涵盖 GZCA 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。

1.2. 文档名称与标识

本文档称作《贵州省电子认证科技有限公司证书策略》（简称“GZCA CP”、“本 CP”），CP 为“Certificate Policy”的缩写。有关本版本 CP 的修订信息请参考附录。本 CP 中为每类证书的证书策略项分配一个唯一的对象标识符，具体可参见本 CP 第 1.4.1 节。

GZCA 向国家 OID 注册管理中心注册了相应的对象标识符（OID），本文档的 OID 为：1.2.156.112660.2.1.1.1.3。

1.3. PKI 参与者

1.3.1. 电子认证服务机构

电子认证服务机构（Certification Authority，简称 CA）是颁发证书的实体。GZCA 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。GZCA 通过给从事电子交易活动的各方主体颁发数字证书、提供证书验证服务等手段而成为电子认证活动的参与主体。CA 是向最终订户或其下 CA 签发证书的实体的术语，它的一个特例是根 CA，一个根 CA 是一类证书体系的最高层。

1.3.2. 注册机构

注册机构（Registration Authority，简称 RA）代表 CA 建立起注册过程，确认证书申请者的身份，批准或拒绝证书申请者。在订户获得证书前，它必须以申请者的身份来注册证书。证书申请者必须从 CA 或 RA 建立的注册过程来完成注册，并将注册信息提交给 CA 或 RA。

CA 或 RA 将对申请者的身份及其它属性进行确认，然后决定是签发还是拒绝该请求。如果签发证书，则证书将被发送给申请者。RA 还可以根据订户需要撤销证书，尽管是 CA 完成最终的撤销工作，并将证书加入到证书撤销列表(CRL)中。

1.3.3. 订户

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

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

1.3.4. 依赖方

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

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。

1.3.5. 其他参与者

其他参与者是指为 GZCA 的电子认证活动提供相关服务的其他实体。

1.4. 证书应用

1.4.1. 适合的应用

GZCA 的订户证书是通用证书，按照证书类型的不同，都有适用的应用。例如个人证书用来发送签名加密邮件、登陆办公 OA 系统等，机构证书用来进行网上申报税等，设备证书用来标识设备身份、进行信息通道加密等。除了因为证书标识的主体身份的不同而导致证书应用差异外，GZCA 订户证书可以广泛应用在电子政务、电子商务及其他社会化活动中，以实现身份认证、电子签名、关键数据加密等目的。法律法规和国家政策有限制的除外。

GZCA 订户证书，从功能上可以满足下列安全需要：

1）身份真实性，保证采用 GZCA 信任服务的证书持有者身份的合法性。

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

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

4）抗抵赖性，对信任体交易不可抵赖性的依据即数字签名进行验证。

根据证书类型，GZCA 所签发的证书包括 SSL 服务器证书、代码签名证书、文档签名证书、E-mail 证书、设备证书、时间戳证书等。

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

1.4.1.1. 个人证书

个人证书即颁发给个人的数字证书，用于区分、标识、鉴别个人身份的应用场合，个人包括自然人或特定身份的人员，如公务员、企业员工、企业法人等。

该类型证书通常用于数字签名、加解密、安全电子邮件以及网上身份认证等，在不违背相关法律法规、本 CP、CPS 以及订户协议的情况下，此类证书也可用于其他用途。

1.4.1.2. 机构证书

机构证书即颁发给机构的数字证书，用于区分、标识、鉴别机构身份的应用场合，机构包括企事业单位、政府机关、社会团体等。

该类型证书通常用于数字签名、加解密以及网上身份认证等，在不违背相关法律法规、本 CP、CPS 以及订户协议的情况下，也可用于其他用途。

1.4.1.3. 设备证书

设备证书即颁发给设备的数字证书，设备包括服务器、防火墙、路由器等，该类证书通常用于网上设备的身份认证，设备之间安全信息的传递。

1.4.1.4. SSL 服务器证书

SSL 服务器证书即颁发给 web 网站或 web 服务器的数字证书，用于标识 Web 网站或者 Web 服务器的身份或资质、提供 SSL/TLS 加密通道，该类证书包含通配型证书、多域名证书类型。

该类证书适合应用在网上银行、电子商务、电子政务、企业信息化以及公共服务等各领域，用于在订户浏览器与 Web 服务器之间建立安全通道，实现数据信息在客户端与服务器之间的加密传输，防止数据信息的泄露；订户或依赖方可

以通过服务器证书验证所访问的网站是否真实可靠，实现网站身份的真实性确认；不得用于各类交易、支付的签名或验证。

GZCA 所签发的 SSL 服务器类证书包括以下四种：

1) EV SSL 证书（Extended Validation SSL Certificates），即扩展验证型服务器证书；
2) OV SSL 证书（Organization Validation Certificates），即需要验证网站所有机构真实身份的标准型 SSL 证书；
3) IV SSL 证书（Individuals Validation SSL Certificates），即需要验证网站经营者个人身份的标准型 SSL 证书；
4) DV SSL 证书（Domain Validation SSL Certificates），即只验证网站域名所有权的简易型 SSL 证书。

其中，EV SSL 证书是经严苛的身份验证后签发的一种扩展型服务器证书，其验证方式符合 CA/浏览器论坛发布的增强型身份验证标准。OV SSL 证书、IV SSL 证书可实现网站机密信息的加密以及网站身份的验证功能，DV SSL 证书只提供网站机密信息的加密功能。

SSL 服务器证书不限制域名的种类，如商业域名、政府域名等。

1.4.1.5. 代码签名证书

代码签名证书即颁发给代码拥有者的数字证书，用于标识软件代码的来源或者所有者，只能用于各类代码的数字签名，不得用于各类交易、支付、加密等应用。GZCA 的代码签名证书签发给机构和个人，分别对应为 OV 代码签名证书和 IV 代码签名证书。

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

1.4.1.6. 邮件证书

邮件证书即颁发给邮件用户的数字证书，将邮件地址与和证书申请者信息进行绑定，以实现邮件地址拥有者的身份认证，以及邮件传输中信息的加解密、签名等操作。

GZCA 所签发的邮件证书包括 DV 邮件证书、IV 邮件证书和 OV 邮件证书。

DV 邮件证书仅验证 E-mail 地址的所有权或控制权，不对 E-mail 地址所有者的身份进行验证，可以确保 E-mail 传输过程中不被他人阅读及篡改，确保 E-mail 内容的完整性。

IV 邮件证书除验证 E-mail 地址的所有权或控制权外，还需验证该 E-mail 地址所属个人使用者身份的真实性。

OV 邮件证书除验证 E-mail 地址的所有权或控制权外，还需验证该 E-mail 地址所属机构身份的真实性。

该类型证书只能用于对电子邮件进行数字签名并加密传输，不得用于各类交易、支付的签名及验证。

1.4.1.7. 事件证书

GZCA 事件证书是 GZCA 的一项扩展业务。

GZCA 事件证书是一种适用于对即时业务或者特定场景业务进行签名认证的数字证书。在业务结束时自动申请，将业务场景中所有信息整合形成数字证书的扩展域信息。使用事件证书对即时业务或者场景业务证据签名后可证明证据在取证结束后无篡改，并保证多个证据之间的关联性和一致性。

GZCA 所签发的事件证书包括 DV 事件证书、IV 事件证书和 OV 事件证书。

DV 事件证书仅验证事件发生行为的真实性，不对行为所有者的身份进行验证。

IV 事件证书除验证事件发生行为的真实性外，还需验证该行为所属个人身份的真实性。

OV 事件证书除验证事件发生行为的真实性外，还需验证该行为所属机构身份的真实性。

事件证书使用时限制签名次数（一次一签），但不限定特定文档，可用于对即时业务或者场景业务中的所有证据进行数据签名。脱离该场景后，证书即不能使用。

1.4.1.8. IOT 设备证书

GZCA IOT 设备证书是 GZCA 的一项扩展业务。

GZCA IOT 设备证书是订户通过物联网申请的用于标识物联网设备的数字证书。

该类证书通常用于物联网设备的身份认证，设备之间安全信息的传递。

1.4.1.9. 时间戳证书

时间戳证书即颁发给时间戳的数字证书，时间戳就是能表示其他的数据在某个特定时间之前已经完整存在、 并且可以验证的一种数据，一般是一个字符序列，能唯一地标识某一刻的时间。适用于需要对数据产生的时间进行认证，从而验证这段数据在产生后是否经过篡改的场景应用。时间戳服务的提供者必须保证服务中使用的时间源是可信的，所提供的时间戳服务是安全的。

目前 GZCA 只签发 OV 时间戳证书，主要用于时间戳服务器，提供数字签名服务。

OV 时间戳证书需验证申请机构身份的真实性。

1.4.1.10. 文档签名证书

文档签名证书即颁发给文档拥有者的数字证书，适用于需要确保文档的真实性、完整性和机密性的场景应用。GZCA 的文档签名证书签发给机构和个人，分别对应为 OV 文档签名证书和 IV 文档签名证书。

OV 文档签名证书需要对机构身份真实性进行验证；IV 文档签名证书需要对个人的身份真实性进行验证。

1.4.1.11. 云端签名证书

GZCA 云端签名证书是 GZCA 的一项扩展业务。

GZCA 云端签名证书是订户通过云服务设备申请的用于云服务场景中进行身份认证或数字签名的数字证书，GZCA 云端签名证书须由终端和签名服务云端协同配合才能完成可靠的数字签名。

GZCA 的云端签名证书签发给机构和个人，分别对应为 OV 云端签名证书和 IV 云端签名证书。

该类型证书通常用于在云服务环境中所进行的数字签名以及身份认证等，在不违背相关法律法规、本 CP、CPS 以及订户协议的情况下，也可用于其他用途。

1.4.1.12. 各类证书的证书策略对象标识符

在本 CP 中为每类证书的证书策略项分配一个唯一的对象标识符，具体如下：

证书类型	证书策略对象标识符
个人证书	1.2.156.112660.1.1.1.2.1
机构证书	1.2.156.112660.1.1.1.3.1
设备证书	1.2.156.112660.1.1.1.4.1
DV SSL 证书	1.2.156.112660.1.1.1.5.1
IV SSL 证书	1.2.156.112660.1.1.1.5.2
OV SSL 证书	1.2.156.112660.1.1.1.5.3
EV SSL 证书	1.2.156.112660.1.1.1.5.4
IV 代码签名证书	1.2.156.112660.1.1.1.6.1
OV 代码签名证书	1.2.156.112660.1.1.1.6.2
DV 邮件证书	1.2.156.112660.1.1.1.7.1
IV 邮件证书	1.2.156.112660.1.1.1.7.2
OV 邮件证书	1.2.156.112660.1.1.1.7.3
DV 事件证书	1.2.156.112660.1.1.1.8.1
IV 事件证书	1.2.156.112660.1.1.1.8.2

OV 事件证书	1.2.156.112660.1.1.1.8.3
IOT 设备证书	1.2.156.112660.1.1.1.9.1
OV 时间戳证书	1.2.156.112660.1.1.1.10.1
IV 文档签名证书	1.2.156.112660.1.1.1.11.1
OV 文档签名证书	1.2.156.112660.1.1.1.11.2
IV 云端签名证书	1.2.156.112660.1.1.1.12.1
OV 云端签名证书	1.2.156.112660.1.1.1.12.2

1.4.2. 限制的证书应用

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

证书不设计用于、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。

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。

任何 GZCA 不认可的证书应用都将不受 GZCA 的保护。

1.5. 策略管理

1.5.1. 策略文档管理机构

GZCA 安全策略委员会是 GZCA 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。

GZCA 安全策略委员会由来自于公司管理层、财务部、市场部、技术部、运营部、客户服务部、行政部等拥有决策权的合适代表组成

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

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。

1.5.2. 联系人

1.5.2.1. 证书问题报告

证书问题报告及证书撤销请求须通过以下方式提交，且证书撤销请求必须以书面形式提交：

发邮件至：apply@gzca.cn.

1.5.2.2. CP 问题

本 CP 在 GZCA 网站发布，对具体个人和组织不另行通知。

任何有关 CP 的问题、建议、疑问等，都可以按以下方式进行联系。

联系人：GZCA 行政管理部门。

网站地址：https://www.gzca.cn。

电子邮箱地址：gzca@gzca.cn。

联系地址： 中华人民共和国贵州省贵阳市高新区长岭南路 178 号茅台国际商务中心（B）-1-12-1。

邮编：550081。

电话号码：+86-851-85559301。

传真号码：+86-851-85559784。

1.5.3. 决定 CP 符合策略的机构

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

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

1.5.4. CP 批准程序

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

1.5.5. CP 修订

GZCA 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。

GZCA 根据国家的政策法规、技术要求、标准的变化及业务发展情况及时修订本 CP， CP 编写小组根据相关的情况拟定 CP 修订建议，提交 GZCA 安全策略委员会审核，经该委员会批准后，正式在 GZCA 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。

1.6. 定义和缩写

1.6.1. 术语定义一览表

术语	定义
GZCA	贵州省电子认证科技有限公司的简称。
GZCA 安全策略委员会	GZCA 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。
本地注册受理点	本地注册受理点（Local Registration Authority）是受理证书服务的终端机构，是GZCA认证服务体系架构内直接面向用户的服务主体，经CA或RA的授权从事各类证书服务。
证书	使用数字签名的电子文件，用于将公钥与身份绑定。
证书策略	一套命名的规则集，用以指明证书对一个特定团体和（或者）具有相同安全需求的应用类型的适用性。例如，一个特定的CP可以指明某类证书适用于鉴别从事企业到企业

	（B-to-B）交易活动的参与方，针对给定价格范围内的产品和服务。
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（电子签名制作数据）	在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。
公钥（电子签名验证数据）	是指订户验证电子签名的数据。
订户	申请证书的实体。
依赖方	依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的个人或机构。
WebTrust	针对电子认证服务机构的现行国际审计标准。

1.6.2. 缩略语及其含义一览表

GZCA	GuiZhou Electronic Certificate CO.,LTD.	贵州省电子认证科技有限公司
KMC	Key Management Center	密钥管理中心
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
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
IETF	The Internet Engineering Task Force	互联网工程任务组
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
SCA	State Cryptography Administration	国家密码管理局
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)
X.509		国际电信同盟认证体系的证书标准
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

2.1. 信息库

GZCA 信息库是一个对外公开的信息库，它能够保存、取回证书及与证书有关的信息。

GZCA 信息库内容包括但不限于以下内容：CP 和 CPS 现行和历史版本、证书、CRL、订户协议，以及其它由 GZCA 在必要时发布的信息。GZCA 将及时发布包括证书、CPS 修订和其它资料等内容。GZCA 信息库可以通过网址：https://www.gzca.cn 查询，或由 GZCA 随时指定的其它通讯方法获得。

2.2. 信息的发布

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

GZCA 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 GZCA 的官网获取证书的信息和撤销证书列表；同时，GZCA 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，GZCA 也将会根据需要采取其他可能的形式进行信息发布。

2.3. 发布的时间和频率

GZCA 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。

ROOTCA（SM2）证书签发的中级 CA 所签发的订户证书，CRL 发布周期为 8 小时，CRL 有效周期最长不超过 24 小时。

在紧急的情况下，GZCA 可以自行决定证书和 CRL 的发布时间。GZCA 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 GZCA 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。

2.4. 信息库访问控制

GZCA 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。

GZCA 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。

3. 身份标识与鉴别

3.1. 命名

3.1.1. 命名类型

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

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

3.1.2. 对命名有意义的要求

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

3.1.3. 订户的匿名或伪名

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。

3.1.4. 解释不同命名的规则

依 X.500 甄别名命名规则解释。

3.1.5. 命名的唯一性

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

3.1.6. 商标的识别、鉴别与角色

GZCA 签发的证书的主体甄别名中不包含商标名。

3.2. 初始身份确认

3.2.1. 证明拥有私钥的方法

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 GZCA 要求的其它证明方式，包括提交 GZCA 发放的初始化信息（被分配的密钥存储介质和对应的 PIN 码）等。

3.2.2. 个人身份的鉴别

个人身份的鉴别包括如下内容：

1）确认申请者身份的真实性和有效性。确认的方式必须是获得申请者至少一种由政府机构颁发的、有效的、带照片的身份证明文件（如居民身份证、护照、军官证或其他同等证照），GZCA 检查该证明文件是否有任何篡改或伪造的痕迹，必要时，GZCA 可以通过签发有效身份证明文件的权威第三方数据库进行核查，确认申请者身份。

2）通过语音通话、视频、邮件等方式与申请者个人进行身份和申请信息的确认，核实证书申请的真实性。

3）确认申请者的地址（如证书主题中包含地址）。GZCA 可以通过物业费账单、银行卡账单或信用卡账单等核实申请者的地址或直接依赖政府签发的身份证明文件上的地址。

4）当申请信息包含机构信息时，需要确认该机构是否存在，以及申请人是否属于该机构的成员，并取得足够的授权。如要求提交任职证明文件、查询第三方数据库、电话确认、发送确认电子邮件等。

5）在域名、设备名称或邮件地址被作为证书主题内容申请证书时，还需要验证该申请者个人是否拥有该权利。

如果认为有需要，GZCA 还可以通过从第三方获取的信息来验证该申请者个人的身份， 如果 GZCA 无法从第三方得到所有所需的信息，可委托第三方进行调查，或要求申请者提供额外的信息和证明材料。

此外，必要时，GZCA 还可以设定其它所需要的鉴别方式和资料。

申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。GZCA在进行了法律规定的有限审查以后，不承担对申请者的身份证明文件进行合法性甄别的义务。

3.2.3. 机构身份的鉴别

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

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

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

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

4. 订户可采用面对面或者邮政信函等方式提交政府机构签发的有效文件。

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

此外，必要时，GZCA 还可以设定其它所需要的鉴别方式和资料。

申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。GZCA在进行了法律规定的有限审查以后，不承担对申请者的身份证明文件进行合法性甄别的义务。

3.2.4. 设备身份的鉴别

设备身份的鉴别会根据其设备拥有者的不同而不同，GZCA 必须对订户进行身份鉴证，包括如下内容：

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

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

如果认为有需要，GZCA 还可以通过从第三方获取的信息来验证该申请者个人的身份， 如果 GZCA 无法从第三方得到所有所需的信息，可委托第三方进行调查，或要求申请者提供额外的信息和证明材料。

此外，必要时，GZCA 还可以设定其它所需要的鉴别方式和资料。

申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。GZCA 在进行了法律规定的有限审查以后，不承担对申请者的身份证明文件进行合法性甄别的义务。

3.2.5. SSL 服务器身份的鉴别

根据所签发的证书类型的不同执行不同的鉴别方式，包括如下内容：

对于 DV SSL 证书，只需验证个人或机构对网站域名的所有权或使用权， 无需对机构或个人的真实身份进行验证，验证方式按照本 CP 第 3.2.10 节执行。

对于 OV SSL 证书，需执行以下验证：

1）验证申请者机构的真实身份及地址验证方式按照本 CP 第 3.2.3 节执行。

2）如申请域名 SSL 证书，按照本 CP 第 3.2.10 节执行对该域名的验证。

3）如申请 IP 地址 SSL 证书，按照本 CP 第 3.2.1 3 节执行对 IP 地址的验证 。

4）如证书中主题中包含机构商业名称，按照本 CP 第 3.2.11 节执行对机构商业名称的验证。

5）确认申请的真实性。通过已验证过的邮箱、电话等，与申请者确认证书申请请求。

6）授权的确认。按照本 CP 第 3.2.16 节执行 。

对 IV SSL 证书，需执行以下验证：

1）验证网站申请者个人的真实身份及地址，其验证方式按照本 CP 第 3.2.2 节执行。

2）如申请域名 SSL 证书，需按照本 CP 第 3.2.10 节执行对该域名的验证。

3）如申请 IP 地址 SSL 证书，需按照本 CP 第 3.2.13 节执行对 IP 地址的验证。

4）确认证书申请请求。 GZCA 通过语音、视频、电话、邮件等方式，与申请者核实证书请求。

对于 EV SSL 证书，需执行以下验证：

1）验证申请者机构的真实身份及地址。验证方式按照本 CPS 第 3.2.3 节执行。

2）验证所申请的域名。验证方式按照本 CP 第 3.2.10 节执行。

3）如证书中主题中包含机构商业名称。按照本 CP 第 3.2.11 节执行对机构商业名称的验证。

4）验证申请者运营存在。通过注册或登记机构的信息记录、权威第三方数据库等进行核实。

5）验证企业主要负责人。通过权威第三方数据库验证主要负责人的身份信息，并通过已验证的联系方式与申请机构确认主要负责人的职位、授权等。

6）如域名申请者与域名所有者不一致，则需提 供域名所有者的授权使用证明文件，GZCA 也可以通过电话、邮箱等方式与域名所有者进行确认。

7）确认申请的真实性。通过已验证过的邮箱、电话等，与申请者确认证书申请请求。

8）授权的确认。同本 CP 第 3.2.1 6 节。

EV SSL 证书不签发 IP 地址证书和通配符证书，不对 IP 地址及通配符域名进行验证。

如果认为有需要，GZCA 还可以通过从第三方获取的信息来验证该申请者个人的身份，如果 GZCA 无法从第三方得到所有所需的信息，可委托第三方进行调查，或要求申请者提供额外的信息和证明材料。

此外，必要时， GZCA 还可以设定其它所需要的鉴别方式和资料。

申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。GZCA 在进行了法律规定的有限审查以后，不承担对申请者的身份证明文件进行合法性甄别的义务。

3.2.6. 代码签名身份的鉴别

根据所签发的证书类型的不同执行不同的鉴别方式，包括如下内容：

对于 IV 文档签名证书订户，GZCA 需按本 CP 第 3.2.2 节的要求完成对个人身份的鉴别。

对于 OV 文档签名证书订户，GZCA 需按本 CP 第 3.2.3 节的要求完成对机构身份的鉴别。

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

3.2.7. 文档签名证书身份的鉴别

根据所签发的证书类型的不同执行不同的鉴别方式，包括如下内容：

对于 IV 文档签名证书订户，GZCA 需按本 CP 第 3.2.2 节的要求完成对个人身份的鉴别。

对于 OV 文档签名证书订户，GZCA 需按本 CP 第 3.2.3 节的要求完成对机构身份的鉴别。

3.2.8. 邮件证书身份的鉴别

根据所签发的证书类型的不同执行不同的鉴别方式，包括如下内容：

对于 DV 邮件证书订户，GZCA 向所申请的 E-mail 地址发送校验码，并收到使用该校验码的确认回复，验证申请者对 E-mail 地址的所有权或控制权。

对于 IV 邮件证书订户，GZCA 除执行基础 E-mail 证书订户的验证流程外，还需按本 CP 第 3.2.2 节的要求完成对个人身份的鉴别。

对于 OV 邮件证书订户，GZCA 除执行基础 E-mail 证书订户的验证流程外，还需按本 CP 第 3.2.3 节的要求完成对机构身份的鉴别

3.2.9. 时间戳证书身份的鉴别

GZCA 只针对机构签发 OV 时间戳证书，OV 时间戳证书身份的鉴别方式按照本 CP 第 3.2.3 节执行。

3.2.10. IOT 设备证书身份的鉴别

根据所签发的证书类型的不同执行不同的鉴别方式，包括如下内容：

对于 IV IOT 设备证书订户，GZCA 需按本 CP 第 3.2.2 节的要求完成对个人身份的鉴别。

对于 OV IOT 设备证书订户，GZCA 需按本 CP 第 3.2.3 节的要求完成对机构身份的鉴别。

对于 CMIOT 设备证书订户，GZCA 需按本 CP 第 3.2.4 节的要求完成对机构身份的鉴别。

3.2.11. 事件证书身份的鉴别

根据所签发的证书类型的不同执行不同的鉴别方式，包括如下内容：

对于 DV 事件证书订户，仅保障签名文档的真实性，不对证书持有者的身份进行鉴别。

对于 IV 事件证书订户，GZCA 需按本 CP 第 3.2.2 节的要求完成对个人身份的鉴别。

对于 OV 事件证书订户，GZCA 需按本 CP 第 3.2.3 节的要求完成对机构身份的鉴别。

3.2.12. 云端协同证书身份的鉴别

根据所签发的证书类型的不同执行不同的鉴别方式，包括如下内容：

对于 IV 云端签名证书订户，GZCA 需按本 CP 第 3.2.2 节的要求完成对个人身份的鉴别。

对于 OV 云端签名证书订户，GZCA 需按本 CP 第 3.2.3 节的要求完成对机构身份的鉴别。

3.2.13. 域名的确认和鉴别

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

1）通过该域名注册服务机构或权威第三方数据库中查询到的该域名持有者登记的电子邮件， 通过邮件的方式发送随机值，并收到使用该随机值的确认回复，确认其对域名的所有权或控制权。鉴别方式遵循 Baseline Requirments v1.7.0 第 3.2.2.4.2 节。

2）向域名联系人发送构建邮件， 通过将一封包含随机值的邮件发送给由‘admin’，‘administrator’，‘webmaster’，‘hostmaster’或‘postmaster’作为前缀加上符号@，以授权域名为尾缀的邮箱，并收到使用该随机值的确认回复，确认其对域名的所有权或控制权。鉴别方式遵循 Baseline Requirments v1.7.0 第 3.2.2.4.4 节。

3）在包含 FQDN（完全限定域名）的 URI（统一资源标识符）的在线网页上对约定的信息进行改动，通过此方式以确认申请者对 FQDN 的实际控制权。鉴别方式遵循 Baseline Requirments v1.7.0 第 3.2.2.4.6 节。【该方法已于 2020 年 6 月 3 日起被禁止使用，因此 GZCA 不再使用该方法】

4）通过确认申请域名在 DNS CNAME、TXT 或 CAA 记录中的任意值或请求令牌的存在来确认申请人对 FQDN(完全限定域名)的控制。鉴别方式遵循 Baseline Requirments v1.7.0 第 3.2.2.4.7 节。

5）通过确认请求值或随机值出现于某个文件的内容中（例如，某个请求值或随机值不出现于用于收取该文件的请求中，并收从请求中收到成功的 HTTP 2xx 状态代码回复），以确认申请者对 FQDN 的实际控制权。该鉴别方式遵循 Baseline Requirments v1.7.0 第 3.2.2.4.18 节。

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

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

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

3.2.14. 机构商业名称验证

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

1）申请者所在辖区的政府机构提供的可证明申请者合法成立、存在或认可的文档，或与该政府机构沟通；

2）可靠的数据来源；

3）与负责管理此类 DBA 名称或商业名称的政府机构沟通；

4）附带支持文件的证明函件；

5）物业账单，银行对账单，信用卡对账单，政府签发的税单，或其他 GZCA 认为可靠的验证方式。

3.2.15. 所在国的确认与鉴别

若证书主题项中包含国家选项，GZCA 通过权威第三方数据库查询网站 DNS 记录显示的

IP 地址或申请者的 IP 地址来确认所在国，确保申请人的 IP 地址所在国与申请人实际所在国一致。

3.2.16. IP 地址的确认和鉴别

GZCA 采用以下方式，确认申请者拥有或实际控制该 IP 地址：

1）在包含 IP 地址的 URI（统一资源标识符）的在线网页上对约定的信息进行改动，通过此方式以确认申请者对 IP 地址的实际控制权。鉴别方式遵循 Baseline Requirments v1.6.6 第 3.2.2.5.1 节。

GZCA 不可为 IP 地址签发 EV SSL 证书。

3.2.17. 数据来源的准确性

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

1) 所提供信息的年限；

2) 信息来源更新的频率；

3) 数据供应商，及数据搜集的目的；

4) 数据对公众的可用性及可访问性；

5) 伪造或更改数据的相对难度。

对于 GZCA 所签发的 SSL 证书，若从评估为可依赖数据来源中获得的数据或文件不超过证书签发前 825 天，则 GZCA 可使用该数据及文件。对于 GZCA 所签发的非 SSL 证书，若从评估为可依赖数据来源中获得的数据或文件的时间不超过本 CP 规定的证书最大有效期，则 GZCA 可使用该数据及文件。

3.2.18. 没有验证的订户信息

证书中的信息必须经过验证，未经验证的信息不得写入证书。

3.2.19. 授权确认

当机构订户授权经办人办理证书业务时，GZCA 应进行如下验证：

1) 通过第三方身份证明服务或数据库、政府主管部门签发的文件等方式确认该机构存在；

2) 通过机构授权文件、电话、有回执的邮政信函、雇佣证明或任何同等方式来验证该人属于上述机构以及其代表行为被该机构授权。

GZCA 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 GZCA 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，GZCA 应向申请者提供其已授权人员的清单。

3.2.20. 互操作准则

对于其他的电子认证服务机构，可以与 GZCA 进行互操作，但是该电子认证服务机构的

CPS 必须符合 GZCA CP 要求，并且与 GZCA 签署相应的协议。

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

如果国家法律法规对此有规定，GZCA 将严格予以执行。

截至目前，GZCA 未签发任何交叉证书。

3.3. 密钥更新请求的标识与鉴别

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。

3.3.1. 常规密钥更新的标识与鉴别

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

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，GZCA 将不承担责任。

对于事件证书，GZCA 不提供密钥更新服务。

3.3.2. 撤销后密钥更新的标识与鉴别

证书撤销后不能进行密钥更新。

3.4. 撤销请求的标识与鉴别

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

4. 证书生命周期操作要求

4.1. 证书申请

4.1.1. 证书申请实体

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

4.1.2. 注册过程与责任

1) 注册过程

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

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

RA 必须对申请信息和申请者的资料进行鉴别

在 RA 向 CA 发送证书请求时，保证传输信息过程安全、保密、完整。

2) 责任

GZCA 及注册机构有责任向订户告知数字证书和电子签名的使用条件；

GZCA 及注册机构有责任向订户告知服务收费的项目和标准；

GZCA 及注册机构有责任向订户告知保存和使用订户信息的权限和责任；

GZCA 及注册机构有责任向订户告知 GZCA 的责任范围；

GZCA 及注册机构有责任向订户告知订户的责任范围；

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

订户负有在其证书申请中提供准确信息的责任；

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

4.2. 证书申请处理

4.2.1. 执行识别与鉴别

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

在签发证书前，GZCA 根据本 CP 3.2.17 的规则确认是否重用此前已验证的信息。

4.2.2. 证书申请批准和拒绝

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

4.2.2.1. 证书申请的批准

如果符合下述条件，RA 可以批准证书申请：

1) 该申请完全满足本 CP 第 3.2 节关于订户身份的标识和鉴别规定；

2) 申请者接受或者没有反对订户协议的内容和要求；

3) 申请者已经按照规定支付了相应的费用。

4.2.2.2. 证书申请的拒绝

如果发生下列情形，RA 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) GZCA 或者注册机构认为批准该申请将会对 GZCA 带来争议、法律纠纷或者损失。

如果法律法规明确禁止某个申请，或 GZCA 认为批准该申请具有高风险性，GZCA 应拒绝该申请，GZCA 根据反钓鱼联盟、防病毒厂商或相关联盟、负责网络安全事务的政府机构等第三方发布的名单，或公共媒体公开报道中披露的信息，或 GZCA 之前由于怀疑网络钓鱼或其他诈骗用途或顾虑而拒绝的证书请求或撤销的证书，建立和维护证书高风险申请人列表，在接受证书申请时将会查询该列表信息。对于列表中出现的申请人，GZCA 将直接拒绝其申请。

对于拒绝的证书申请，GZCA 通知申请者证书申请失败。

4.2.3. 处理证书申请的时间

GZCA 的电子认证业务规则（CPS）应规定合理的证书申请处理时间。GZCA 和注册机构应在 CPS 规定的时间内处理证书申请，无论是批准还是拒绝。这个时间通常是 2-3 个工作日。

4.2.4. 认证机构授权（CAA）

对于 GZCA 颁发 SSL/TLS 证书，GZCA 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。

GZCA 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“GZCA.com.cn”，则 GZCA 不签发对应的证书；若 CAA 记录中出现“iodef”标签，则 GZCA 与申请者沟通后决定是否为其颁发证书。

GZCA 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 GZCA 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。

4.3. 证书签发

4.3.1. 证书签发中 RA 和 CA 的行为

根 CA 的证书签发应由 GZCA 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。

在证书的签发过程中 RA 的管理员负责证书申请的审批，并通过操作 RA 系统将签发证书的请求发往 CA 的证书签发系统。RA 发往 CA 的证书签发请求信息须有 RA 的身份鉴别与信息保密措施，并确保请求发到正确的 CA 证书签发系统。

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

4.3.2. CA 和 RA 通知订户证书的签发

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

4.4. 证书接受

4.4.1. 构成接受证书的行为

1) 订户自行访问专门的 GZCA 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) GZCA 注册机构在订户的允许下，代替订户下载证书，并把证书通过邮件及其他 GZCA 认为可靠方式发送给订户，即代表订户接受了证书。

3) 订户接受了获得证书的方式，并且没有提出反对证书或者证书中的内容。

4.4.2. CA 对证书的发布

订户接受证书后，GZCA 将该订户证书发布到 GZCA 的目录服务系统。

4.4.3. CA 通知其他实体证书的签发

除证书订户外，GZCA 及注册机构不需要通知其他实体证书的签发。

4.5. 密钥对和证书的使用

4.5.1. 订户私钥和证书的使用

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

对于签名证书，其私钥可用于对信息的签名，订户应知悉并确认签名的内容。对于加密证书，其私钥可用于对采用对应公钥加密的信息进行解密。在证书到期或被撤销之后，订户必须停止使用该证书对应的私钥。

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

4.5.2. 依赖方公钥和证书的使用

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 GZCA 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。

4.6. 证书更新

证书更新指在不改变证书中订户的公钥或其他任何信息的情况下，为订户签发一张新证书。

4.6.1. 证书更新的情形

对于 GZCA 签发给订户的证书，订户需在证书到期前进行证书更新。GZCA 根据本 CP3.2.17 的规则确认是否重用此前已验证的信息。证书过期后，订户必须重新申请新证书。

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

4.6.2. 请求证书更新的实体

请求证书更新的实体为证书订户。

4.6.3. 处理证书更新请求

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

1）订户的原证书存在并且由 GZCA 所签发；

2）验证证书更新请求在许可期限内；

3）基于原注册信息进行身份鉴别。

在以上验证和鉴别通过后 GZCA 才可批准签发证书。

订户也可以选择一般的初始证书申请流程进行证书更新，按照要求提交相应的证书申请和身份证明资料。GZCA 在任何情况下都可将这种初始证书申请的鉴别方式作为证书更新时的鉴别处理手段。

4.6.4. 通知订户新证书的签发

同本 CP 第 4.3.2 节。

4.6.5. 构成接受更新证书的行为

同本 CP 第 4.4.1 节。

4.6.6. CA 对更新证书的发布

同本 CP 第 4.4.2 节。

4.6.7. CA 通知其他实体证书的签发

同本 CP 第 4.4.3 节。

4.7. 证书密钥更新

证书密钥更新指订户或其他参与者生成一对新密钥并申请为新公钥签发一个新证书。

4.7.1. 证书密钥更新的情形

GZCA 的证书密钥更新包括但不限于以下情形：

1) 证书私钥泄露而撤销证书；

2) 证书到期；

3) 基于技术、政策安全原因，GZCA 要求证书密钥更新。

4.7.2. 请求证书密钥更新的实体

请求证书密钥更新的实体为证书订户。

4.7.3. 处理证书密钥更新请求

同本 CP 第 4.6.3 节。

4.7.4. 通知订户新证书的签发

同本 CP 第 4.3.2 节。

4.7.5. 构成接受密钥更新证书的行为

同本 CP 第 4.4.1 节。

4.7.6. CA 对密钥更新证书的发布

同本 CP 第 4.4.2 节。

密钥更新证书应在 24 小时内发布。

4.7.7. CA 通知其他实体证书的签发

同本 CP 第 4.4.3 节。

4.8. 证书变更

4.8.1. 证书变更的情形

如果订户提供的注册信息发生改变，必须向 GZCA 提出证书变更。

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

证书变更的申请和证书申请所需的流程、条件是一致的。

4.8.2. 请求证书变更的实体

请求证书变更的实体为证书订户。

4.8.3. 处理证书变更请求

证书变更按照初次申请证书的注册过程进行处理，同本 CP 3.2。

4.8.4. 通知订户新证书的签发

同本 CP 第 4.3.2 节。

4.8.5. 构成接受变更证书的行为

同本 CP 第 4.4.1 节。

4.8.6. CA 对变更证书的发布

同本 CP 第 4.4.2 节。

4.8.7. CA 通知其他实体证书的签发

同本 CP 第 4.4.3 节。

4.9. 证书撤销和挂起

4.9.1. 证书撤销的情形

4.9.1.1. 订户证书撤销的原因

若出现以下情况中的一种或多种，GZCA 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 GZCA 最初的证书请求未得到授权且不能追溯到授权行为；

3) GZCA 获得了证据，证明与证书公钥对应订户私钥遭到了泄漏；

4) GZCA 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）证书不再符合本 CP 第 6.1.5 节及第 6.1.6 节；

2）GZCA 获得了证书遭到误用的证据；

3）GZCA 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）GZCA 获悉了任何表明 FQDN 或 IP 地址的使用不再被法律许可（例如，某法院或仲裁员已经撤销了域名注册人使用域名的权力，域名注册人与申请人的相关许可及服务协议被终止，或域名注册人未成功更新域名）；

5）GZCA 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）GZCA 获悉证书中所含信息出现重大变化；

7）GZCA 获悉证书的签发未能符合 GZCA 的 CP 或 CPS；

8）GZCA 认为任何或被告知出现在证书中的信息为错误信息；

9）GZCA 从事电子认证业务的资格失效，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） GZCA 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。

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

1）CA 与 RA、受理点等签订的协议终止或者发生改变；

2）证书私钥发生安全性损害或者被怀疑发生安全性损害；

3）出于管理的需要。

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

1）CA 机构得知域名不在合法，如被法院判定该域名非法、与域名注册机构的合约终止等；

2）CA 机构得知一个通配符证书被用来验证一个欺诈性的误导子域名；

3）CA 机构由于某种原因终止运行，并且未安排其他 CA 提供撤销证书的支持性操作；

4）CA 签发证书的权利已届满或被撤销或终止，除非 CA 已作出安排，继续维护 CRL/OCSP；

5）证书的技术内容或格式造成了对应用软件供应商或依赖方不可接受的风险。

4.9.1.2. 中级 CA 证书的撤销原因

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

1）GZCA 获得了证据，证明与证书公钥对应的中级 CA 私钥遭到了损害，或不再符合本 CP 第 6.1.5 节及第 6.1.6 节的相关要求；

2）GZCA 获得了证书遭到误用的证据；

3）GZCA 获悉证书的签发未能符合 CP/CPS；

4）GZCA 认为任何出现在中级 CA 证书中的信息不准确、不真实或具有误导性；

5）GZCA 由于任何原因停止运营，且未与另一家 CA 达成协议以提供证书撤销服务；

6）GZCA 从事电子认证业务的资格失效，或被撤销或被终止，除非其继续维护 CRL/OCSP 信息库。

4.9.2. 请求证书撤销的实体

以下实体可以请求撤销一个订户证书：

1）GZCA 或注册机构可以依据本 CP 第 4.9.1 节要求撤销一个订户证书；

2）对于个人证书，证书订户可以请求撤销他们自己的个人证书；

3）对于机构证书，只有机构授权的代表有资格请求撤销已经签发给该机构的证书；

4）对于设备证书，只有拥有设备的机构授权的代表有资格请求撤销已经签发的证书；

5）法院、政府主管部门及其他公权力部门可以依法撤销订户证书。

6）依赖方、应用软件提供商、防病毒机构或其他的第三方可以提交证书问题报告，告知 GZCA 有合理理由撤销证书。

只有 GZCA 可以撤销根证书或者中级 CA 证书。

4.9.3. 证书撤销请求的处理程序

4.9.3.1. 订户请求撤销证书

1）订户向注册机构提交撤销，同时说明撤销原因；

2）注册机构核实申请撤销实体的身份和撤销理由的正当性；

3）注册机构将撤销申请表提交给 GZCA，由 GZCA 完成撤销。

4）GZCA 提供 7*24 小时的撤销申请服务。

4.9.3.2. 订户被强制撤销证书

1）当 GZCA 或注册机构有充分的理由确信出现本 CP 第 4.9.1.1 节中的情况时，可通过内部确定的流程撤销证书；

2）GZCA 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，GZCA 应组织调查并根据调查结果来决定是否撤销证书；

4）GZCA 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。

4.9.4. 撤销请求的宽限期

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。

4.9.5. CA 处理撤销请求的时限

GZCA 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。

4.9.6. 依赖方检查证书撤销的要求

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

4.9.7. CRL 发布频率

对于 ROOTCA（SM2）证书签发的中级 CA 所签发的订户证书，CRL 发布周期为 8 小时，CRL 有效周期最长不超过 24 小时。

对于中级 CA 证书，GZCA 的 CRL 发布周期为 12 个月。如果撤销中级 CA 证书，GZCA 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 GZCA 制定的发布策略决定。

4.9.8. CRL 发布的最大滞后时间

一个证书从它被撤销到它被发布到 CRL 上的滞后时间不能超过 24 小时。

4.9.9. 在线状态查询的可用性

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

4.9.10. 在线状态查询要求

用户可以自由进行在线状态查询，GZCA 不得设置任何的读取权限。

GZCA 提供 Get 和 Post 两种方式的 OCSP 查询服务。

对于订户证书，GZCA 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，GZCA 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，GZCA 不得返回“good”状态 。

4.9.11. 撤销信息的其他发布形式

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

4.9.12. 密钥损害的特别要求

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 GZCA 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。

4.9.13. 证书挂起的情形

GZCA 不支持证书挂起。

4.9.14. 请求证书挂起的实体

GZCA 不支持证书挂起。

4.9.15. 挂起请求的程序

GZCA 不支持证书挂起。

4.9.16. 挂起的期限限制

GZCA 不支持证书挂起。

4.10. 证书状态服务

4.10.1. 操作特征

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，GZCA 不应在证书到期前删除其在 CRL 中的撤销记录。GZCA 不删除 CRL 中代码签名证书的撤销记录。

GZCA 不删除 OCSP 中的撤销记录。

4.10.2. 服务可用性

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。

4.10.3. 可选特征

不适用。

4.11. 订购结束

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。

4.12. 密钥托管与恢复

4.12.1. 密钥托管与恢复的策略与行为

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

证书订户的加密密钥对由 GZCA 代订户向贵州省密钥管理中心申请生成，并由贵州省密钥管理中心进行管理。当证书订户需要恢复加密密钥时，按照贵州省密钥管理中心的规范、流程，接受订户的申请，为订户恢复相应的加密密钥。

对于 SSL 服务器证书和代码签名证书，GZCA 不提供代订户生成签名密钥对的操作。

除云端签名证书外，GZCA 不提供订户私钥的托管和恢复服务。

4.12.2. 会话密钥的封装与恢复的策略与行为

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

5. 认证机构设施、管理和操作控制

5.1. 物理控制

5.1.1. 场地位置与建筑

GZCA 机房位于贵州省贵阳市高新区长岭南路 178 号，机房电磁屏蔽效能满足 BMB3-1999 标准“C”级要求。机房具备抗震、防火、防水、恒湿温控、独立供电、门禁控制、视频监控等功能，可保证认证服务的连续性和可靠性。

GZCA 中心机房按照功能主要分为核心区、服务区、操作区、公共区四个区域。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。屏蔽门是电动平移屏蔽门。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。

5.1.2. 物理访问控制

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。GZCA 的 CPS 必须对物理访问控制进行比较详细的规定。

5.1.3. 电力与空调

GZCA 机房配有安全、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。

5.1.4. 防水

GZCA 机房有专门的技术措施，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。

5.1.5. 火灾防护

GZCA 机房采取预防措施，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。

5.1.6. 介质存放

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。

5.1.7. 废物处理

当 GZCA 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。

5.1.8. 异地备份

GZCA 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。

5.2. 程序控制

5.2.1. 可信角色

在 GZCA 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 GZCA 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。

5.2.2. 每项任务需要的人数

GZCA 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。

GZCA 对于人员有明确的分工，贯彻互相牵制、互相监督的安全机制。

5.2.3. 每个角色的识别与鉴别

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 GZCA 的人员聘用管理条例中规定。

5.2.4. 需要职责分割的角色

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。

5.3. 人员控制

5.3.1. 资格、经历和清白要求

GZCA 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 GZCA 的统一安排及管理；

3）遵守 GZCA 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。

7）关键和核心岗位的工作人员必须具有足以胜任其工作的相关经验，且没有相关的不良记录，或通过 GZCA 相关的培训和考核后方能上岗。

GZCA 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。

5.3.2. 背景调查程序

GZCA 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。对于公开信任证书业务的关键岗位必须进行全面调查。

调查程序包括：

1）人事部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。

2）人事部门通过电话、信函、网络、走访等形式对其提供的材料的真实性进行鉴定。

3）在背景调查中，对发现以下情形的人员，可以直接拒绝其成为可信人员的资格：

①. 存在捏造事实或资料的行为；

②. 借助不可靠人员的证明；

③. 使用非法的身份证明或者学历、任职资格证明；

④. 工作中有严重不诚实的行为。

4）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。

5）经考核，GZCA 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，GZCA 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。

5.3.3. 培训要求

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

1）GZCA 颁布的证书策略和电子认证业务规则；

2）PKI 基本知识；

3）国家关于电子认证服务的法律、法规及标准、程序等；

4）GZCA 运营体系、技术体系和安全管理制度；

5）工作职责和岗位说明；

6）其他需要进行的培训等。

5.3.4. 再培训的频度和要求

GZCA 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。

5.3.5. 工作岗位轮换的频度和次序

GZCA 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。

5.3.6. 未授权行为的处罚

GZCA 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。

5.3.7. 独立合约人的要求

对于不属于 GZCA 机构内部工作人员，但从事 GZCA 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，GZCA 的统一要求如下：

1）人员档案的备案管理，包括提供身份证、学历证书、资格证书、无犯罪记录等有效证明，并需与 GZCA 签署保密协议；

2）GZCA 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 GZCA 证书受理规则和电子认证业务规则。

5.3.8. 提供给人员的文件

GZCA 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。

5.4. 审计记录程序

5.4.1. 记录事件的类型

CA 和 RA 必须记录与运行系统相关的事件。这些记录，无论是手动生成或者是系统自动生成，都应该包含以下信息：

1）事件发生的日期和时间；

2）记录的序列号；

3）记录的类型；

4）记录的来源；

5）记录事件的实体。

GZCA 应记录的事件包括但不限于：

1） CA 密钥生命周期内的管理事件，包括 CA 密钥生成、备份、存储、恢复、使用、撤销、归档、销毁、私钥泄露等；

2） 证书生命周期内的管理事件，包括证书的申请、批准、更新、撤销等；

3） 密码设备生命周期内的管理事件，包括设备的采购、接收、安装、卸载、激活、使用、维修、解除运作及弃用；

4） RA 系统记录的证书订户身份信息；

5） 系统、网络安全事件，包括：成功或不成功访问 CA 系统的活动，系统日常运行产生的日志文件，系统变更等；

6） 信息安全设备的安全事件；

7） 系统操作事件，包括系统权限的创建、删除，设置或修改密码；

8） 认证机构设施的访问，包括授权人员进出认证机构设施、非授权人员进出认证机构设施等相关记录；

9） 可信人员管理记录，包括系统权限的创建、删除及变更等；

10）其他不符合规程的事件。

5.4.2. 处理日志的频度

GZCA 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。

5.4.3. 审计日志的保留期限

GZCA 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。

5.4.4. 审计日志的保护

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。

5.4.5. 审计日志的备份程序

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。

5.4.6. 审计收集系统

不适用。

5.4.7. 对导致事件主体的通知

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。

5.4.8. 脆弱性评估

根据审计记录，GZCA 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。

5.5. 记录归档

5.5.1. 归档记录的类型

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，包括但不限于：

1) 证书申请信息；

2) 证书签发过程中的支持文档；

3) 电子认证业务规则、证书策略、管理制度等；

4) 员工资料，包括但不限于员工信息、背景调查、培训、录用离职等资料；

5) 审计记录；

6) 各类外部、内部审查评估文档。

5.5.2. 归档记录的保留期限

GZCA 的电子认证业务规则（CPS）应规定合理的归档记录保留期限。

5.5.3. 归档文件的保护

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。

5.5.4. 归档文件的备份程序

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。

5.5.5. 记录时间戳要求

GZCA 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。

5.5.6. 归档收集系统

各自实体应在内部建设归档收集系统，包括 GZCA 和注册机构。

5.5.7. 获得和检验归档信息的程序

GZCA 的安全审计员和运维人员分别保留归档信息的 2 个拷贝。在获得完整归案信息时， 须对这 2 个拷贝进行比较。

5.6. 密钥变更

在 CA 证书到期时，GZCA 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，GZCA 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。

在生成新的 CA 密钥对时，必须严格遵守 GZCA 关于密钥管理的规范。新的密钥对产生时，GZCA 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。

CA 密钥更替时，必须保证整个证书链的顺利过渡。

5.7. 损害与灾难恢复

5.7.1. 事故和损害处理程序

GZCA 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。

5.7.2. 计算机资源、软件和/或数据的损坏

如果出现计算机资源、软件和/或数据损坏的事件，GZCA 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。

5.7.3. 实体私钥损害处理程序

在故意的、人为的或是自然灾难的情况下，GZCA 将采取下列步骤以恢复安全环境：

1） GZCA 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 GZCA 业务操作员的配置文件，则由另外一名 GZCA 安全业务操作员或业务管理员对其进行恢复。

当 CA 根私钥出现损毁、遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，GZCA 将启动重大事件应急处理程序，由安全策略委员会和相关专家进行评估，并制定行动计划。如果需要注销 CA 证书，将会采取以下措施：

1） 立即向政府主管部门汇报，通过电话、网站和其它公共媒体对订户和依赖方进行通告，采取措施避免用户利益遭受更大损失；

2） 立即撤销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。同时 GZCA 立即生成新的密钥对，并自签发新的根证书；

3）新的根证书签发以后，按照本 CP 关于证书签发的规定，重新签发下级证书；

4）新的根证书签发以后，将会立即通过信息库、目录服务器、HTTP 等方式进行发布；

5）重新为订户签发证书。

5.7.4. 灾难后的业务存续能力

GZCA 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。

5.8. CA 或 RA 的终止

当 GZCA 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 GZCA 终止前，必须：

1）委托业务承接单位；

2）起草 GZCA 终止声明；

3）通知与 GZCA 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 GZCA 业务管理员和 GZCA 业务操作员的操作权限；

地址：中国贵州省贵阳市长岭南路178号 邮编：550081
电话：+86-851-85559301 传真：+86-851-85559784
网址：https://www.gzca.cn

11） 处理加密密钥；

12） 处理和存储敏感文档；

13） 清除 GZCA 主机硬件。

当 RA 因故终止服务时，GZCA 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。

6. 认证系统技术安全控制

6.1. 密钥对的生成与安装

6.1.1. 密钥对的生成

6.1.1.1. CA 密钥对生成

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、备份和恢复应遵循国家密码管理局的相关规定。用于此类密钥生成的密码模块须通过国家密码主管部门鉴定、认证。

CA 密钥对的生成过程需录像或由一名合格的审计师见证以确保其遵循 CP 以及角色分离的要求。密钥对生成过程和操作均需记录并保存。

6.1.1.2. 订户密钥对生成

根据业务发展需要，GZCA 可以签发双密钥证书（密钥对包括签名密钥对和加密密钥对）或单密钥证书（签名和加密使用同一对密钥）。GZCA 订户的加密密钥对由 GZCA 代订户向贵州省密钥管理中心申请生成，并由贵州省密钥管理中心进行管理。当证书订户需要恢复加密密钥时，按照贵州省密钥管理中心的规范、流程，接受订户的申请为订户恢复相应的加密密钥。对于单密钥证书订户，GZCA 不提供加密密钥对生成服务。

订户密钥对的产生，必须遵循国家的法律政策规定。GZCA 支持多种模式的签名密钥对产生方式，可以使用硬件密码模块（如：USB Key），也可以使用国家密码管理局批准的软件密码模块，也可以使用标准的软件密码模块（如：Web 服务器软件提供的密钥生成功能等），证书申请者可根据其需要进行选择。不管何种方式，密钥对产生的安全性都应该得到保证。

GZCA 在技术、业务流程和管理上，已经实施了安全保密的措施。

对于 SSL/TLS 证书、时间戳证书、设备证书，订户的密钥对由订户自己生成并保管。

对于 IOT 设备证书、邮件证书、事件证书、云端签名证书，GZCA 允许订户在线生成密钥对并将私钥加密保护后通过安全通道传送给订户，或由订户提交 CSR 签发证书。

对于代码签名证书、文档签名证书，由订户采用符合标准要求的硬件设备（如 USBKey 或加密机）或受签名人控制的其他安全方式生成密钥对。如采用硬件设备生成密钥对，则生成的私钥不能复制和导出，同时必须使用口令激活私钥，GZCA 通过安全通道将激活口令传递给订户。

GZCA 一般不提供代为生成签名密钥对，如果用户书面申请并经 GZCA 批准，GZCA 可以为申请者代为生成密钥对，并且承诺不保留私钥的副本，采取足够的措施保证密钥对的安全性、可靠性和唯一性，但是由于此密钥对的遗失、泄露等原因造成的损失，GZCA 不承担任何责任与义务。

证书订户负有保护私钥安全的责任和义务，并承担由此带来的法律责任。

6.1.2. 私钥传送给订户

由订户自己生成时，签名证书对应的私钥将不会进行传送。

订户委托 GZCA 产生签名密钥对时，签名证书对应的私钥生成时将采用离线或者在线安全方式传递，GZCA 确保私钥在交给客户前未被使用，并且承诺不保留私钥的备份，但是由于此私钥的遗失、泄露等原因造成的损失，GZCA 不承担任何责任与义务。

订户的加密证书对应的私钥由证书签发机构代替订户对密钥管理中心提出加密密钥申请请求，密钥管理中心对产生的加密私钥使用订户通讯密钥进行数字信封加密，以数据流的方式传送给证书签发机构，通过证书签发机构下载到订户证书载体时，订户使用自己的证书载体解密该私钥并存储。

对于需要传递私钥的证书，私钥加密保护后通过安全通道传送给订户。

6.1.3. 公钥传送给证书签发机构

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 GZCA 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）。

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 GZCA 签发，GZCA 在签发证书前验证所提交请求中的订户签名。

6.1.4. CA 公钥传送给依赖方

GZCA 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。

GZCA 也需要通过目录发布其 CA 证书。

6.1.5. 密钥的长度

GZCA 支持的 SM2 密钥长度至少为 256 位，支持的 RSA 密钥长度为 2048 位或以上。

如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，GZCA 将会完全遵从。

6.1.6. 公钥参数的生成和质量检查

对于使用硬件密码模块的 GZCA 订户，公钥参数必须使用国家密码主管部门批准许可的加密设备和硬件介质生成，例如加密机、加密卡、USB Key、IC 卡等生成和选取，并遵从这些设备的生成规范和标准。GZCA 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。

6.1.7. 密钥使用目的

GZCA 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 GZCA 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 7.1.2。

6.2. 私钥保护和密码模块工程控制

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。

6.2.1. 密码模块的标准和控制

GZCA 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 FIPS140-2 第三级别的技术要求，订户使用的密码模块符合 FIPS-2 第二级别的技术要求。

6.2.2. 私钥多人控制（m 选 n）

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 3，n 不小于 2。

6.2.3. 私钥托管

不适用。

6.2.4. 私钥备份

为了保证业务持续开展，GZCA 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。

对于订户签名证书，如果其私钥存放在软件密码模块中，建议订户对私钥进行备份，备份的私钥需要采用口令保护等授权访问控制，防止非授权的修改或泄露。

对于订户加密证书，其加密私钥由密钥管理中心进行备份，备份私钥以密文形式存在。

6.2.5. 私钥归档

在 CA 私钥到期后，必须使用满足 CP 第 6.2.1 节要求的硬件密码模块归档保存至少 7 年。归档期限结束后，对 CA 私钥的销毁应符合 CP 第 6.2.10 节的规定。

6.2.6. 私钥导出、导入密码模块

CA 的私钥，GZCA 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。

GZCA 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。

6.2.7. 私钥在密码模块的存储

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 FIPS140-2 三级标准或同等安全水平。

订户的私钥存储在符合国家密码管理规定的 USB Key 介质或文件证书中，所有在 USB Key 中存储的私钥，都以密文的形式保存。对于使用软件密码模块生成的私钥，最好在硬件密码模块中存储和使用（硬件密码模块至少符合 FIPS140-2 二级标准或同等安全水平），订户也可以自主选择使用有安全保护措施的特定软件密码模块。

6.2.8. 激活私钥的方法

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。

对于存放在诸如 USB Key、加密卡、加密机或者其他形式的硬件密码模块中的订户私钥，订户可以通过口令、IC 卡等方式进一步保护。当订户计算机上安装了相应的驱动后，将 USB Key、IC 卡等插入相应设备中，输入保护口令，则私钥被激活。对于存放在订户计算机软件密码模块中的私钥，订户应该采用合理的措施从物理上保护计算机，以防止在没有得到用户授权的情况下，其他人员使用订户的计算机和相关私钥。如果存放在软件密码模块中的私钥没有口令保护，那么软件密码模块的加载意味着私钥的激活。如果使用口令保护私钥，软件密码模块加载后，还需要输入口令才能激活私钥。

6.2.9. 冻结私钥的方法

一旦私钥被激活，除非这种状态被冻结，私钥总是处于活动状态。在某些私钥的使用当中，私钥每次被激活，只能进行一次操作，如果需要进行第二次操作，需要再次进行激活。

冻结私钥的方式包括退出登陆状态、切断电源、将硬件密码模块移开、注销用户或系统等。

对于 CA 私钥，当存放私钥的设备断电，私钥就被冻结。

订户冻结私钥由其自行决定，当每次操作后注销计算机，或者把硬件密码模块从读卡器中取出，切断电源时，私钥就被冻结。

6.2.10. 解除私钥激活状态的方法

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。

对于最终订户加密证书私钥，在其生命周期结束后，应该妥善保存一定期限，以便于解开加密信息。对于最终订户签名证书私钥，在其生命周期结束后，如果无需再保存，由订户决定其销毁方法，可以通过私钥的删除、系统或密码模块的初始化、物理销毁私钥存储模块等方式来销毁。

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。

6.2.11. 密码模块的评估

GZCA 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，GZCA 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。

6.3. 密钥对管理的其他方面

6.3.1. 公钥归档

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。

6.3.2. 证书操作期和密钥对使用期限

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。

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

另外需注意的是无论是订户证书还是 CA 证书，证书到期后，在保证安全的情况

对于不同的证书，其密钥对允许通过证书更新的最长使用期限如下：

1）对 ROOTCA（SM2）签发的 SM2 CA 证书，其密钥对的最长允许使用年限是 20 年，可少于 20 年；

2）对 GZCA SM2 签发的 SM2 CA 证书，其密钥对的最长允许使用年限是 20 年，可少于 20 年；

3）对 GZCA 的 RSA4096 位根 CA 证书，其密钥对的最长允许使用年限是 30 年，可少于 30 年；

4）对 GZCA Root RSA 签发的 RSA4096 位 CA 证书，其密钥对的最长允许使用年限是 30 年，可少于 30 年；

5）对 GZCA RSA 签发的 RSA2048 位 CA 证书，其密钥对的最长允许使用年限是 13 年，可少于 13 年；

6）对于个人证书、机构证书，其密钥对的最长允许使用年限是 5，可少于 5 年；

7）对于设备证书，其密钥对的最长允许使用年限是 10 年，可少于 10 年；

8）对于代码签名证书，其密钥对的最长允许使用期限是 39 个月，可少于 39 个月；

9）对于文档签名证书、邮件证书，其密钥对的最长允许使用年限是 3 年，可少于 3 年；

10） 对于 IOT 设备证书、云端签名证书，其密钥对的最长允许使用年限是 1 年，可少于 1 年；

11） 对于时间戳证书，其密钥对的最长允许使用年限是 10 年，可少于 10 年；

12) 对于 SSL/TLS 服务器证书，其密钥对的最长允许使用期限是397天，可少于397天；

13) 对于事件证书，其密钥对的最长允许使用期限是3天，可少于3天。

6.4. 激活数据

6.4.1. 激活数据的产生和安装

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。

订户私钥的激活数据，包括用于下载证书的口令（以密码信封的形式提供）、USB Key 的 PIN 码等，都必须在安全可靠的环境下随机产生。

6.4.2. 激活数据的保护

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。

对于订户私钥的激活数据，包括口令或 PIN 码，都必须在安全可靠的环境下产生。订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。同时为了配合业务系统的安全需求，应该经常对激活数据进行修改。

6.4.3. 激活数据的其他方面

当私钥的激活数据进行传送时，应保护它们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

当私钥的激活数据不需要时应该销毁，并保护它们在此过程中免于丢偷窃、泄露或非授权使用，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或全部，比如记录有口令的纸页必须粉碎。

6.5. 计算机安全控制

6.5.1. 特别的计算机安全技术要求

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

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。

6.5.2. 计算机安全评估

GZCA 的认证系统，通过了国家密码管理局的安全性审查。

6.6. 生命周期技术控制

6.6.1. 系统开发控制

GZCA 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，GZCA 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。

6.6.2. 安全管理控制

GZCA 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。

GZCA 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。GZCA 还对认证系统进行定期和不定期的检查和测试。

GZCA 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。

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。

GZCA 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。

6.6.3. 生命周期的安全控制

GZCA 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。

6.7. 网络的安全控制

GZCA 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，GZCA 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。

6.8. 时间戳

GZCA 遵循 RFC 3161、5816 时间戳协议标准提供时间戳服务，采用标准的时间戳请求、时间戳应答以及时间戳编码格式，时间源采用国家授时中心提供的标准时间。

7. 证书、证书撤销列表和在线证书状态协议

7.1. 证书描述

GZCA 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）。

GZCA 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。

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。

表 7-1 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
公钥	根据 RFC 5280 编码，使用 CP 第 7.1.3 节中指定的算法，密钥长度满足 CP第 6.1.5 节指定的要求

7.1.1. 版本号

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

7.1.2. 证书扩展项

GZCA 除了使用 X.509 V3 版证书标准扩展项以外，还使用了自定义扩展项。自定义扩展项的使用是允许的，但是除非由于特别应用而包含该项，不保证该扩展项的使用。

7.1.2.1. 标准扩展项

1） 密钥用法（key usage）

指定证书密钥对的用法：电子签名，不可抵赖，密钥加密，数据加密，密钥协议，验证证书签名，验证 CRL 签名，只加密，只解密，只签名。

2） 颁发机构密钥标识符（authority Key Identifier）

最终订户证书及中级 CA 证书加入颁发机构密钥标识符扩展项，当证书签发者包含主题密钥标识扩展项时，颁发机构密钥标识符由 160 位的颁发证书机构的公钥进行 SHA-1 散列运算后的值构成。否则，它将包含颁发 CA 的主题 DN。这个扩展项的 criticality 域设置为 FALSE。

3） 主题密钥标识符（subject Key Identifier）

证书的主题密钥标识符扩展项赋值时，证书主题的公钥的密钥标识符被产生。使用该扩展项时，其扩展项的 criticality 域设为 FALSE。

4） CRL 发布点（CRL Distribution Points）

证书中的 CRL 的分发点扩展项，它包含本地的一个链接，可以向依赖方提供 CRL 的信息以便其查询证书状态。此扩展项的 criticality 项应设为 FALSE。

5） 证书策略扩展项（certificate Policies）

证书策略扩展项中有本 CP 中对应证书类的 CP 对象标识符及策略限定符。这个扩展项的 criticality 域设置为 FALSE。

6） 基本限制扩展项（basic Constraints）

CA 证书的基本限制扩展项中的主题类型被设为 CA。最终订户证书的基本限制扩展项的主题类型设为最终实体（End-Entity）。这个扩展项的 criticality 域设置为 FALSE。将来，对于其它的证书，这个扩展项的 criticality 域可以设置为 TRUE。

CA 证书的基本限制扩展项中的路径长度设定为在证书路径中该证书之后的 CA 级数。对于最终订户证书签发 CA，其 CA 证书“path Len Constraint”域的值设为 0，表示证书路径中仅有一个最终订户证书可以跟在这个 CA 证书后面。

7.1.2.2. 自定义扩展项

针对不同的证书应用服务需求，GZCA 灵活定义一些扩展项，包括但不限于如下扩展项：

1) 社会保险号：用于表示订户的社会保险号码。
2) 组织机构代码：用于表示企业组织机构代码。
3) 工商注册号：用于表示企业工商注册号码
4) 国税登记证号：用于表示企业国税号码
5) 信任服务号：证书颁发机构产生用于标识订户的唯一编号。
6) 地税登记证号：用于表示企业地税号码。
7) 个人身份证号码：用于表示居民身份证的唯一编号。

7.1.3. 算法对象标识符

GZCA 签发的 SM2 证书，密码算法的标识符为 SM3WithSM2。

GZCA 签发的 RSA 证书，密码算法的标识符为 SHA256withRSA。

GZCA 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。

7.1.4. 名称形式

GZCA 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。

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。

7.1.5. 名称限制

不适用。

7.1.6. 证书策略对象标识符

当使用证书策略扩展项时，证书中包含证书策略的对象标识符，该对象标识符与相应的证书类别对应。

7.1.7. 策略限制扩展项的用法

不适用。

7.1.8. 策略限定符的语法和语义

不适用。

7.1.9. 关键证书策略扩展项的处理语义

与 X509 和 PKIX 规定一致。

7.2. 证书撤销列表

GZCA 定期签发 CRL，供用户查询使用。

依本 CP 签发的 CRL 符合 RFC5280 标准。CRL 至少包含如下表所述基本域和内容。

域	值或者值的限制
版本	V2
颁发者	签发 CRL 的实体，颁发者甄别。
生效日期	CRL 的签发日期
下次更新	CRL 下次签发的日期。CRL 每隔 24 小时更新
签名算法	签发 CRL 所使用的签名算法
颁发机构密钥标识符	由 160 位的颁发证书机构公钥进行散列运算后的值构成
撤销列表	列出撤销的证书，包括撤销证书的序列号和撤销日期

7.2.1. 版本

GZCA 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。

7.2.2. CRL 和 CRL 条目扩展项

不适用。

7.3. OCSP 描述

GZCA 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。

7.3.1. 版本号

RFC6960 定义的 OCSP 版本。

7.3.2. OCSP 扩展项

不适用。

8. 认证机构审计和其他评估

8.1. 评估的频度和情形

为了检查、确认 GZCA 是否按照其 CP、CPS、业务规范、管理制度和安全策略开展业务，同时发现机构运营过程中存在的可能风险，GZCA 将依照严格的审计方法和审计过程每年对 CA 中心及其注册机构进行定期审计，以评估符合 GZCA 的 CP、CPS 以及相关的规范、操作程序和标准。

除了内部审计和评估外，GZCA 还将聘请第三方独立审计师事务所进行外部审计和评估。

GZCA 在如下情形中进行评估：

1) 根据《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》规定，接受主管部门的评估和检查。
2) GZCA 电子认证系统每年进行信息系统风险评估，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。
3) GZCA 按照国家主管部门的要求、国家相关标准和本 CPS 的规定，对其运营和服务每年进行一致性审计和评估。
4) 按照国家主管部门的要求、国家相关标准、本 CPS 的规定以及公司安全管理策略的要求，每年至少执行一次内部评估审核，包括对 GZCA 在内的其它实体（RA、受理点等） 的评估审核。

评估的频率为：

1) 年度评估：接受主管部门对 GZCA 进行的年度检查；对 GZCA 电子认证系统进行信息系统风险评估；对运营和服务进行一致性审计和评估。
2) 运营前评估：在新系统向公众提供服务之前由行业主管部门对新系统进行评估，评估合格后方可正式运营。

8.2. 评估者的身份/资格

GZCA 的内部审计，由 GZCA 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。

若需邀请外部审计机构对GZCA 进行外部审计和评估,聘请的外部审计机构，应该具备以下资质：

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) 熟悉 IT 运营管理、计算机信息安全体系、通信网络安全要求、公钥基础设施（PKI）技术及相关的法律法规、标准规范要求；
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。

8.3. 评估者与被评估者之间的关系

GZCA 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。

外部评估者（主管部门、审计机构以及其他机构）与 GZCA 之间是独立的关系，没有任何利害关系足以影响评估的客观性，评估人员应以独立、公平、客观的态度对 GZCA 进行评估。

8.4. 评估的内容

GZCA 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。

8.5. 对问题与不足采取的行动

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

第三方审计机构评估完成后，GZCA 按照其工作报告进行整改，并接受再次审计和评估。

8.6. 评估结果的传达与发布

当 GZCA 接受行业主管部门的检查或评估后，行业主管部门会向公众发布对 GZCA 的检查或评估结果。

当 GZCA 进行内部审计和评估后，审计和评估结果将只在公司内部以及涉及的证书注册机构进行传达；对可能造成订户安全隐患的，GZCA 将及时向订户通报。

8.7. 自评估

见章节 8.1。

9. 法律责任和其他业务条款

9.1. 费用

GZCA 可根据提供的电子认证相关服务向本机构的证书订户收取费用，具体费用将取决于市场规则和相关管理部门的规定。

9.1.1. 证书新增和更新费用

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

如果 GZCA 签署的协议中指明的价格和 GZCA 公布的价格不一致，以协议中的价格为准。

9.1.2. 证书查询费用

对于证书查询，目前 GZCA 不收取任何费用。除非用户提出的特殊需求，需要 GZCA 支付额外的费用，GZCA 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，GZCA 将会及时在网站 www.gzca.cn 上予以公布。

9.1.3. 撤销和状态信息查询费用

对于撤销和状态信息查询，目前 GZCA 不收取任何费用。除非用户提出的特殊需求，需要 GZCA 支付额外的费用，GZCA 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 ， GZCA 将会及时在网站 www.gzca.cn 上予以公布。

9.1.4. 其他服务费用

1）如果用户向 GZCA 索取纸质的 CP 或其他相关的作业文件时，GZCA 需要收取因此产生的邮递和处理工本费。

2）GZCA 将向用户提供证书存储介质及相关服务，GZCA 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 GZCA 将要或者可能提供的服务的费用，GZCA 将会及时公布，供用户查询。

9.1.5. 退款策略

GZCA 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，GZCA 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，GZCA 遵守严格的操作程序和策略。如果 GZCA 违背了本 CP 所规定的责任或其它重大义务，订户可以要求 GZCA 撤销证书并退款。在 GZCA 撤销了订户的证书后，GZCA 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，GZCA 将追究其法律责任。

9.2. 财务责任

9.2.1. 保险范围

保险范围主要针对 CP 第 9.9 节中所规定的赔偿。

9.2.2. 其他财产

不适用。

9.2.3. 对最终实体的保险或担保范围

证书订户一旦接受 GZCA 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。

9.3. 业务信息保密

9.3.1. 保密信息范围

在 GZCA 提供的电子认证服务中，以下信息视为保密信息：

1）GZCA 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 GZCA 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 GZCA 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。

9.3.2. 不属于保密的信息

1）由 GZCA 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）。

9.3.3. 保护保密信息的责任

GZCA、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。

当保密信息的所有者出于某种原因，要求 GZCA 公开或披露他所拥有的保密信息时，GZCA 应满足其要求；同时，GZCA 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，GZCA 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。

当 GZCA 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，GZCA 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，GZCA 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。

9.4. 个人隐私保密

9.4.1. 隐私保密计划

GZCA 应制定隐私保密计划对订户的个人信息保密。

9.4.2. 作为隐私处理的信息

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；

2) 订户的联系电话；

3) 订户的地址；

4) 订户的银行帐号。

9.4.3. 不被认为隐私的信息

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。

9.4.4. 保护隐私的责任

GZCA、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。

9.4.5. 使用隐私信息的告知与同意

GZCA 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，GZCA 都没有告知订户的义务， 也无需得到订户的同意。

GZCA 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。

GZCA、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）。

9.4.6. 依法律或行政程序的信息披露

由于法律执行、法律授权的行政执行的需要，GZCA 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。

9.4.7. 其他信息披露情形

如果订户要求 GZCA 提供某类特定客户支援服务如资料邮寄时，GZCA 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。

9.5. 知识产权

1）GZCA 享有并保留对证书以及 GZCA 提供的所有软件的全部知识产权；

2）GZCA 对数字证书系统软件具有所有权、名称权、利益分享权；

3）GZCA 网站上公布的一切信息均为 GZCA 财产，未经 GZCA 书面允许，他人不能转载用于商业行为；

4）GZCA 发行的证书和 CRL 均为受 GZCA 支配的财产；

5）对外运营管理策略和规范为 GZCA 财产；

6）用来表示目录中 GZCA 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 GZCA 的财产。

9.6. 陈述与担保

9.6.1. CA 的陈述与担保

GZCA 对证书订户必须做出如下担保：

1）GZCA 签发给订户的证书符合本 CP 的所有实质性要求；

2）验证证书中所包含的全部信息的准确性（organizationalUnitName 信息除外）；

3）GZCA 保证其私钥得到安全的存放和保护，GZCA 建立和执行的安全机制符合国家相关政策的规定；

4）GZCA 将按本 CP 的规定，及时撤销证书；

5）GZCA 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。

6）验证申请者对列在证书主题字段及主题别名扩展（或，仅针对域名而言，获得了拥有域名使用权或控制权人士的授权）中的域名及 IP 地址拥有使用权或控制权；

7）验证申请者授权了证书的签发以及申请者代表获得了授权，以代表申请者申请证书；

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 CP 3.2 的要求验证申请人的身份；

10） 若 GZCA 与订户无关联，则 GZCA 与订户是合法有效且可执行的订户协议双方；若 GZCA 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。

GZCA 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）GZCA 完全遵照本 CP 及 CPS 的规定签发证书；

3）在 GZCA 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。

9.6.2. RA 的陈述与担保

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 GZCA 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 GZCA 提交证书申请、撤销、更新等服务申请。

9.6.3. 订户的陈述与担保

订户一旦接受 GZCA 签发的证书，就被视为向 GZCA、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 GZCA 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 GZCA 公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等；

9）证书在本 CP 中规定使用范围内合法使用，只将证书用于经过授权的或其他合法的使用目的；

10） 采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件；

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

12） 对于代码签名证书，订户不得将其用于可疑代码等非法软件、恶意软件的签名。

9.6.4. 依赖方的陈述与担保

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 GZCA 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 GZCA 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。

9.6.5. 其他参与者的陈述与担保

遵守本 CP 的所有规定。

9.7. 担保免责

除本 CP 9.6.1 中的明确承诺外，GZCA 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 GZCA 之责任。

9.8. 有限责任

证书订户、依赖方因 GZCA 提供的电子认证服务从事民事活动遭受损失，GZCA 只承担本 CP 第 9.9.1 节规定的有限责任。

9.9. 赔偿

9.9.1. 认证机构的赔偿责任

如 GZCA 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 GZCA 承担赔偿责任（法定或约定免责除外），包括以下情形：

1）GZCA 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，GZCA 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 GZCA 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 GZCA 的原因导致 CA 私钥的泄露；

5）GZCA 未能及时撤销证书，导致依赖方遭受损失的。

9.9.2. 订户的赔偿责任

在如下情况，订户对自身原因造成的 GZCA、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 GZCA 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 GZCA 及其授权的证书服务机构，以及不当交付他人使用造成 GZCA 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 GZCA 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 GZCA 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 GZCA 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 GZCA 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。

9.9.3. 依赖方的赔偿责任

在如下情况，依赖方对自身原因造成的 GZCA、订户损失，应当承担赔偿责任：

1）没有履行 GZCA 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 GZCA 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。

9.10. 有效期与终止

9.10.1. 有效期

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 GZCA 终止电子认证服务时失效。

9.10.2. 终止

GZCA 终止电子认证服务时，本 CP 终止。

9.10.3. 终止的效果与存续

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。

9.11. 对参与者的个别通告及信息交互

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。

9.12. 修订

9.12.1. 修订程序

经 GZCA 安全策略委员会授权，CP 编写小组每年至少审查一次本 CP，确保其符合国家法律法规、主管部门的要求以及相关国际标准，符合认证业务开展的实际需要。

本 CP 的修订，由 CP 编写小组提出修订报告，获得 GZCA 安全策略委员会批准后，由 CP 编写小组负责组织修订，修订后的 CP 经过 GZCA 安全策略委员会批准后正式对外发布。

9.12.2. 通知机制和期限

修订后的 CP 经批准后将立即在 GZCA 的网站 www.gzca.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，GZCA 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。

9.12.3. 必须修订的情形

如果出现下列情况，GZCA 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。

9.13. 争议解决条款

当 GZCA、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。

9.14. 管辖法律

GZCA 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。

9.15. 符合适用法律

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。

9.16. 一般条款

9.16.1. 完整协议

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。

9.16.2. 让渡

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。

9.16.3. 分割性

如果本 CP 的任何条款或其应用由于与 GZCA 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 ，GZCA 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，GZCA 应在此章节批露修订的内容。

9.16.4. 强制执行

不适用。

9.16.5. 不可抗力

依据本 CP 制定的 CPS 应包括不可抗力条款，以保护各方利益。

9.17. 其他条款

GZCA 对本 CP 具有最终解释权。

地址：中国贵州省贵阳市长岭南路178号 邮编：550081
电话：+86-851-85559301 传真：+86-851-85559784
网址：https://www.gzca.cn