

数安时代科技股份有限公司

证书策略和电子认证业务规则

版本：6.7

发布日期：2026 年 10 月 31 日

版本控制表

版本号	修订内容	生效日期
V1.0	发布初版。	2005-7-15
V2.0	调整第九章涉及的费用的描述。	2006-9-30
V3.0	文档的整体调整、更新。	2010-1-1
V3.1/V3.2	更新 1.1.2 节，增加粤港互认项目证书符合的证书策略； 更新第四章证书生命周期涉及的证书变更、吊销和冻结相关的内容； 更新第五章有关物理环境、归档记录、根证书有效期相关的内容； 更新第六章有关计算机安全评估、系统开发控制相关的规则等。	2013-2-21
V3.3	更新版本信息。	2014-7-1
V4.0	增加SSL/TLS、Adobe文档签名、S/MIME安全邮件、代码签名证书相关业务规则。	2014-12-1
V4.1	增加粤港互认项目证书的业务规则； 调整密钥对生成、传送和归档等方面的要求。	2015-5-10
V4.2	增加 SSL/TLS 证书的规则要求； 增加双因素验证机制要求； 增加证书类型及其价格标准和保险范围。	2015-10-1
V4.3	变更文档中涉及的公司名称及相关责任描述； 增加根证书链及相关规则描述。	2016-8-1
V4.4	根据 CA/B 论坛的管理标准要求更新国际业务证书涉及的身份验证、证书生命周期管理、密钥存储及吊销方面的规则要求。	2016-12-1
V4.5	增加英文对照版； 修订粤港互认项目证书身份鉴别方式； 调整 CPS 的生效期限。	2017-5-1
V4.6	调整身份鉴别要求及证书生命周期管理规则； 调整密码长度要求； 补充 GDCA 及订户的陈述与担保等相关内容。	2017-6-1
V4.7	披露“GDCA ROOT CA1 证书”层次架构； 调整域名鉴别相关的验证方式和版本号；	2018-5-1

	调整记录时间戳的要求。	
V4.8	增加适用于 WebTrust 审计范围内的证书相关的规则要求； 明确区分 WebTrust 审计范围内的证书业务及非 WebTrust 审计范围内的证书业务，避免产生混淆或误解； 删除与个人和机构身份鉴别无关的描述。	2018-7-5
V4.9	增加 SSL/TLS 证书相关的规则要求，包括证书问题报告，管理要求的引用等。 调整公开可信订户证书密钥对生成的文字描述。	2018-10-14
V5.0	调整粤港互认项目证书所遵循的策略版本及个人身份鉴别方式； 增加粤港互认项目证书中级 CA 相关规定； 增加时间戳证书有效期规定以及调整设备证书的有效期规定； 调整 SSL/TLS 证书相关的规则要求。	2019-9-25
V5.1	调整域名验证方法； 调整 SSL/TLS 证书的最大有效期和密钥对的最长使用期限； 调整个人及机构证书的最大有效期。	2020-5-31
V5.2	更新域名验证规则； 调整记录事件类型的内容； 调整日志分析的周期。	2020-8-20
V5.3	调整证书问题报告的联系方式； 披露 EV SSL/TLS 证书审核验证所采用的数据来源。	2020-10-1
V5.4	披露 SM2 算法新子 CA 及其密钥对使用期限； 调整保险范围的描述。	2021-2-5
V5.5	披露证明私钥泄露的方法。	2021-5-31
V5.6	披露 RSA 新中级 CA； 区分 WebTrust 审计范围内的证书业务及非 WebTrust 审计范围内的证书业务所涉及的个人和机构证书的 OID； 调整代码签名证书、SSL/TLS 证书相关规则； 披露域名及 IP 地址验证数据重用规则等。	2021-11-1
V5.7	披露两个新中级 CA 及其密钥对使用期限；	2022-7-19

	披露时间戳证书的相关规则。	
V5.8	披露邮件证书的相关规则； 明确 Adobe AATL 个人和机构签名证书的审核验证规则。	2022-10-25
V5.9	明确域名验证中随机值的验证方式及有效期； 明确网络安全控制符合 NCSSR 的要求； 调整证书、CRL 和 OCSP 规则。	2023-5-8
V6.0	根据 CA/B 论坛要求披露符合 S/MIME Requirement 要求的邮件证书相关规则。	2023-8-21
V6.1	调整随机值的最大有效期； SSL/TLS 证书明确 basicConstraints（如出现）为关键扩展项。	2024-4-15
V6.2	调整部分中级 CA 证书的到期时间和签发订户证书的截止日期； 调整证书问题报告联系电话号码； 增加 linting 检测要求； 调整审计日志及归档记录保存期限。	2025-2-28
V6.3	调整域名验证规则； 增加防火墙和路由器活动日志记录要求； 添加披露撤销相关内容； 增加漏洞处理时限管理。	2025-11-5
V6.4	调整 GDCA TrustAUTH R4 Generic CA 证书停止签发用户证书的时限。	2025-12-31
V6.5	披露新中级 CA，并调整部分中级 CA 的用户证书签发时限； 调整 SSL/TLS 证书相关的规则； 调整验证数据最大重用时长。	2026-3-13
V6.6	增加电子认证业务遵循的策略要求； 补充 DNSSEC 验证要求等。	2026-6-5
V6.7	基于 V6.6 版本，对原 CP/CPS 文档按照证书应用场景进行结构化拆分，分别形成适用于 SSL/TLS 证书业务及电子签名认证证书等业务的独立 CP/CPS 文档。 根据《TCQAE 11034-2025 电子认证业务规则规范》要求，重新编制电子签名认证证书业务 CP/CPS，适用于电子签名认证证书业务及部分非签名场景的电子认证服务。	2026-10-31

目录

1. 概括性描述 1

1.1. 承诺 1

1.2. 基本信息 1

1.2.1 GDCA 简介 1

1.2.2 办公场所及联系方式 2

1.2.3 证书策略和电子认证业务规则（CP /CPS） 2

1.2.4 GDCA 证书层次架构 3

1.3. 文档名称与标识 5

1.3.1 证书策略标识 5

1.4. 电子认证活动参与者 5

1.4.1. 电子认证服务机构 5

1.4.2. 订户 5

1.4.3. 依赖方 5

1.4.4. 其他参与者 6

1.5. 证书应用 6

1.5.1. 适合的证书应用 6

1.5.2. 限制的证书应用 9

1.6. 策略管理 9

1.6.1. 策略管理机构 9

1.6.2. 策略文档的批准程序 9

1.7. 定义和缩写 10

1.7.1. 术语定义一览表 10

1.7.2. 缩略语及其含义一览表 11

2. 信息发布与信息管理 11

2.1. GDCA 信息库 11

2.2. 信息的发布 12

2.3. 发布的时间和频率 12

2.4. 信息库访问控制 12

2.5. 信息备案和对接 13

3. 身份标识与查验 13
3.1. 身份查验通用要求 13
3.1.1. 通用要求 13
3.1.2. 订户告知 13
3.2. 初始身份确认 14
3.2.1. 证明拥有私钥的方法 14
3.2.2. 个人身份的查验 14
3.2.3. 机构身份的查验 16
3.3. 订户意愿记录 17
3.3.1. 订户意愿记录内容 17
3.3.2. 个人高等级证书的意愿记录 17
3.3.3. 个人基础级证书的意愿记录 17
3.3.4. 机构高等级证书的意愿记录 18
3.3.5. 机构基础级证书的意愿记录 18
3.4. 设备身份的鉴别 18
3.5. 订户协议 19
3.6. 未验证的订户信息 19
3.7. 互操作要求 19
3.8. 命名 19
3.8.1. 名称类型 19
3.8.2. 对名称意义化的要求 21
3.8.3. 订户的匿名或伪名 21
3.8.4. 理解不同名称的形式的规则 21
3.8.5. 名称的唯一性 21
3.8.6. 商标的识别、鉴别与角色 22
4. 证书生存周期操作要求 22
4.1. 通用要求 22
4.2. 证书申请 22
4.2.1. 证书申请实体 22
4.2.2. 注册过程 22

4.2.3. 证书申请处理 23
4.2.4. 处理证书申请的时间 23
4.3. 证书签发 24
4.3.1. 证书签发过程中认证服务机构的行为 24
4.3.2. 电子认证服务机构和注册机构对订户的通告 24
4.4. 证书接受 24
4.4.1. 构成接受证书的行为 24
4.4.2. 电子认证服务机构对证书的发布 25
4.4.3. 电子认证服务机构对其他实体的通告 25
4.5. 密钥对和证书的使用 25
4.5.1. 订户的私钥和证书的使用 25
4.5.2. 安全事件反馈 26
4.6. 证书续期 26
4.6.1. 证书续期的情形 26
4.6.2. 请求证书续期的实体 27
4.6.3. 证书续期请求的处理 27
4.6.4. 颁发新证书时对订户的通告 27
4.6.5. 构成接受续期证书的行为 27
4.6.6. 电子认证服务机构对续期证书的发布 27
4.6.7. 电子认证服务机构对其他实体的通告 27
4.7. 证书密钥更新 27
4.7.1. 证书密钥更新的情形 27
4.7.2. 请求证书密钥更新的实体 28
4.7.3. 证书密钥更新请求的处理 28
4.7.4. 颁发新证书时对订户的通告 28
4.7.5. 构成接受密钥更新证书的行为 28
4.7.6. 电子认证服务机构对密钥更新证书的发布 28
4.7.7. 电子认证服务机构对其他实体的通告 28
4.8. 证书变更 28
4.8.1. 证书变更的情形 29

4.8.2. 请求证书变更的实体 29
4.8.3. 证书变更请求的处理 29
4.8.4. 颁发新证书时对订户的通告 29
4.8.5. 构成接受变更证书的行为 29
4.8.6. 电子认证服务机构对变更证书的发布 29
4.8.7. 电子认证服务机构对其他实体的通告 29
4.9. 证书撤销或冻结 30
4.9.1. 证书撤销的情形 30
4.9.2. 请求证书撤销的实体 30
4.9.3. 撤销请求的流程 30
4.9.4. 撤销请求宽限期 31
4.9.5. 电子认证服务机构处理撤销请求的时限 32
4.9.6. 依赖方检查证书撤销的要求 32
4.9.7. CRL 发布频率 32
4.9.8. CRL 发布的最大滞后时间 32
4.9.9. 在线状态查询的可用性 33
4.9.10. 在线状态查询要求 33
4.9.11. 撤销信息的其他发布形式 33
4.9.12. 密钥损害的特别要求 33
4.9.13. 证书冻结的情形 33
4.9.14. 请求证书冻结的实体 33
4.9.15. 冻结请求的流程 33
4.9.16. 冻结的期限限制 33
4.10. 证书状态信息服务 33
4.10.1. 证书信息状态服务方式 33
4.10.2. 证书状态信息服务 34
4.10.3. 备用查询机制 34
4.11. 停止使用认证服务 34
4.11.1. 停止使用认证服务的情形 34
4.11.2. 停止服务请求的处理时限和方式 34

4.11.3. 用户数据的保存、销毁与转移 35
4.11.4. 停止服务后的责任延续 35
4.11.5. 操作记录 35
4.12. 密钥托管与恢复 35
5. 认证机构设施、管理和操作控制 35
5.1. 物理控制 35
5.1.1. 场地位置与建筑 35
5.1.2. 物理访问 37
5.1.3. 安防监控 37
5.1.4. 电力与空调 37
5.1.5. 水患防治 38
5.1.6. 火灾防护 38
5.1.7. 存储媒体管理 38
5.1.8. 设备管理 39
5.1.9. 废物处理 39
5.1.10. 异地备份 39
5.2. 操作过程控制 39
5.2.1. 可信角色 39
5.2.2. 职责分离 40
5.3. 人员控制 40
5.3.1. 可信人员资格要求 40
5.3.2. 可信人员培训要求 41
5.4. 审计日志程序 41
5.4.1. 记录事件的内容及范围 41
5.4.2. 审计日志的保存期限 42
5.4.3. 日志审计内容及审计周期 42
5.5. 记录归档 42
5.5.1. 归档记录的类型 42
5.5.2. 归档记录的保存期限 43
5.5.3. 归档文件的保护 43

5.6. 电子认证服务机构根证书密钥更替 43
5.7. 损害与灾难恢复 44
5.7.1. 业务连续性目标 44
5.7.2. 事故和损害处理程序 44
5.7.3. 灾难后的业务连续性能力 45
5.8. 电子认证服务机构终止 45
5.9. 重大事项报告 46
6. 认证系统技术安全控制 47
6.1. 技术安全管理制度要求 47
6.2. 密钥对的生成与安装 47
6.2.1. 根证书密钥对的生成和安装 47
6.2.2. 订户密钥对生成和交付 48
6.3. 私钥保护和密码模块工程控制 49
6.3.1. CA 私钥保护和密码模块工程控制 49
6.3.2. 订户私钥保护和密码模块工程控制 49
6.4. 密钥对管理的其他方面 50
6.4.1. 公钥归档 50
6.4.2. 证书操作期和密钥对使用期限 50
6.5. 激活数据 51
6.5.1. 激活数据的产生和安装 51
6.5.2. 激活数据的保护 51
6.5.3. 激活数据的其他方面 52
6.6. 计算机安全控制 52
6.6.1. 特别的计算机安全技术要求 52
6.6.2. 计算机安全评估 53
6.7. 生存周期技术控制 53
6.7.1. 系统开发控制 53
6.7.2. 安全管理控制 54
6.7.3. 生存周期的安全控制 54
6.8. 网络安全控制 54

6.8.1. 网络结构与边界安全控制 54
6.8.2. 网络访问控制 55
6.8.3. 网络监控与安全审计 55
6.9. 时间戳 55
7. 证书、证书撤销列表和在线证书状态协议 55
7.1. 证书 55
7.1.1. 版本号 56
7.1.2. 证书扩展项 56
7.1.3. 算法对象标识符 59
7.1.4. 名称形式 59
7.1.5. 名称限制 59
7.1.6. 证书策略对象标识符 59
7.1.7. 策略限制扩展项的用法 59
7.1.8. 策略限定符的语法和语义 59
7.1.9. 关键证书策略扩展项的处理规则 59
7.2. 证书撤销列表 59
7.2.1. 版本 60
7.2.2. CRL 和 CRL 条目扩展项 60
7.3. 在线证书状态协议 60
7.3.1. 版本号 61
7.3.2. OCSP 请求和响应处理 61
7.3.3. OCSP 扩展项 62
8. 认证机构审计及相关评估 62
8.1. 审计评估制度 62
8.2. 认证业务审计 62
8.3. 全面符合性评估 63
9. 法律责任和其他业务条款 63
9.1. 费用 63
9.1.1. 证书颁发和更新费用 63
9.1.2. 证书访问及查询费用 63

9.1.3. 证书撤销或状态信息的查询费用 64
9.1.4. 电子签名相关费用 64
9.1.5. 其他服务费用 64
9.1.6. 退款策略 64
9.2. 财务责任 65
9.2.1. 保险范围 65
9.2.2. 其他资产 65
9.2.3. 对最终实体的保险或担保 65
9.2.4. 责任免除 66
9.3. 业务信息保密 67
9.3.1. 保密信息范围 67
9.3.2. 不属于保密的信息 67
9.3.3. 保护保密信息的责任 67
9.4. 个人隐私保护 67
9.4.1. 隐私保密方案 67
9.4.2. 作为隐私处理的信息 68
9.4.3. 不被视为隐私的信息 68
9.4.4. 保护隐私的责任 69
9.4.5. 使用隐私信息的告知与同意 69
9.4.6. 依法律或行政程序的信息披露 69
9.4.7. 其他信息披露情形 69
9.5. 知识产权 69
9.6. 陈述与担保 70
9.6.1. 电子认证服务机构的陈述与担保 70
9.6.2. 注册机构的陈述与担保 70
9.6.3. 订户的陈述与担保 71
9.6.4. 依赖方的陈述与担保 71
9.6.5. 其他参与者的陈述与担保 72
9.7. 担保免责 72
9.8. 偿付责任规则 72

9.9. 赔偿 73
9.10. 有效期限与终止 73
9.10.1. 有效期限 73
9.10.2. 终止 73
9.10.3. 效力的终止与保留 74
9.11. 对参与者的个别通告与沟通 74
9.12. 修订和发布 74
9.12.1. 修订程序 74
9.12.2. CP/CPS 修订 74
9.12.3. 通知机制和期限 75
9.12.4. 必须修改 OID 的情形 75
9.13. 争议处理与举证 75
9.14. 管辖法律 76
9.15. 与适用法律的符合性 76
9.16. 一般条款 76
9.16.1. 完整协议 76
9.16.2. 转让 76
9.16.3. 分割性 77
9.16.4. 强制执行（律师费用和权利放弃） 77
9.16.5. 不可抗力 77
9.17. 其他条款 77

1. 概括性描述

1.1. 承诺

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”）承诺：

（1）在开展电子认证经营和服务活动时，遵守《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证业务规则规范》、《电子政务电子认证服务管理办法》、《电子认证服务密码管理办法》等法律、法规，树立以人民为中心的服务理念，承担社会责任。

（2）与客户建立业务关系前，开展应用业务调研，深入了解其业务性质、商业模式、应用场景、目标用户群体以及业务流程。基于调研结果，确定业务风险等级。建立应用接入业务风险评估及内部定责机制，明确在客户准入和风险评估中，各部门的职责和审批权限，禁止为存在违法违规风险的业务提供电子认证服务。

（3）使用经过国家密码管理局审查的电子认证服务系统开展电子认证服务。

（4）接受政府和社会监督，主动配合主管部门（如工业和信息化部、国家密码管理局等）的例行检查、专项检查等，对主管部门检查发现的问题及时整改；建立畅通的投诉举报渠道，对外公布监督方式，认真处理订户、合作方、依赖方等反馈的问题。按要求建立问题纠治长效机制，持续符合整改要求，确保 GDCA 始终能处于合规状态。

1.2. 基本信息

1.2.1 GDCA 简介

数安时代（法定代表人：徐莉萍）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：ECP44010220007；批准日期：2005 年 9 月 6 日；目前许可证有效期为 2020 年 9 月 6 日至 2025 年 9 月 5 日。）的电子认证服务机构之一；2008 年 12 月，获得国家密码管理局颁发的《商用密码产品销售许可证》；2011 年 4 月，通过了国家密码管理局电子政务电子认证服务能力评估，获得《电子政务电子认证服务机构》（编号：A021）资格。2013 年，对电子认证服务系统进行 SM2 算法升级，并通过了国家密码管理局组织的安全性审查。2015 年，GDCA 通过了 WebTrust 国际安全审计认证，具备了国际标准化的运营管理和服务水平，可以提供全球化的电子认证服务。为适应业务发展需要，2016 年 5

月，“广东数字证书认证中心有限公司”更名为“数安时代科技股份有限公司”。2017 年 8 月 11 日，GDCA 在新三板挂牌交易，股票简称：数安时代，股票代码：871932。

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。

1.2.2 办公场所及联系方式

注册地：广东省佛山市南海区狮山镇南海软件科技园科教路（广东省数字证书认证中心）

广州市办公场地：广东省广州市越秀区越华路 112 号珠江国际大厦 30 楼 3001 室

电话号码：020-83487228

邮政编码：510030

佛山市办公场地：广东省佛山市南海区桂城街道港口路 12 号三山科创中心 C6 座 11 楼

电话号码：0757-85132828

邮政编码：528200

电子邮箱地址：gdca@gdca.com.cn

网站地址：https://www.gdca.com.cn/

1.2.3 证书策略和电子认证业务规则（CP /CPS）

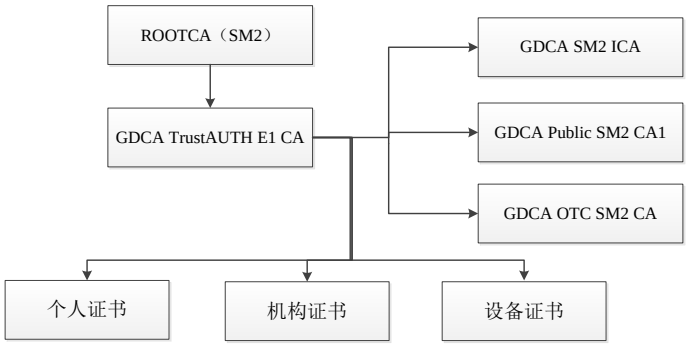
本证书策略和电子认证业务规则（简称 CP/CPS）根据《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》、《TCQAE-11034-2025 电子认证业务规则规范》等法律法规的要求，详细阐述了 GDCA 提供的电子认证服务整个过程、电子认证服务所遵循的策略、规则以及电子认证服务相关参与者所承担的责任。本 CP/CPS 由 GDCA 通过公开发布的形式告知电子签名订户、依赖方和其他相关参与者，以确保 GDCA 所提供的电子认证服务是合法、专业、权威的第三方电子认证服务。对于 GDCA 所提供电子认证服务过程的责任范围，本 CP/CPS 也给予了明确的规定。

本 CP/CPS 中所涉及的粤港电子签名互认证书，同时也遵循《粤港电子签名证书互认证书策略（1.1 版本）》（http://gdii.gd.gov.cn/xxh3236/content/post_945261.html）。证书是否应用于粤港跨境互认项目可根据证书策略的对象标识符进行辨别。

1.2.4 GDCA 证书层次架构

本 CP/CPS 涵盖 2 个根证书，分别为 ROOTCA 证书（SM2）、GDCA ROOT CA1 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。

（1） ROOTCA (SM2）



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

ROOTCA 证书（SM2）将于 2042 年 7 月 7 日到期。

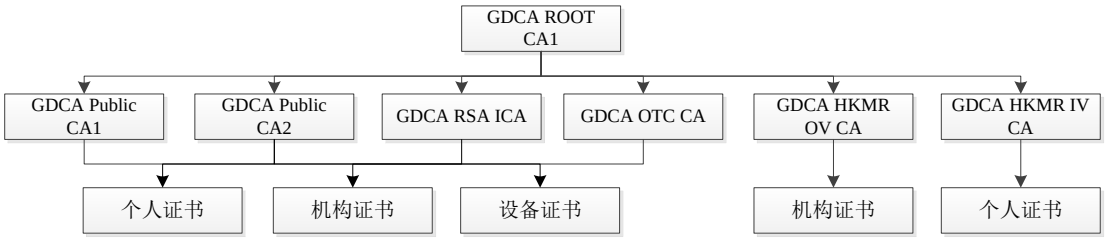
Guangdong Certificate Authority（GDCA TrustAUTH E1 CA）证书将在 2034 年 6 月 21 日到期，2030 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

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

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

GDCA OTC SM2 CA 证书将在2033年8 月22日到期，2030 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

（2） GDCA ROOT CA1



GDCA ROOT CA1 证书是 GDCA 自签根证书，根密钥长度为 4096-bit，下设 6 个中级 CA 证书，其中：（1）GDCA Public CA1，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的个人证书、机构证书、设备证书；（2）GDCA Public CA2，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的个人证书、机构证书、设备证书；（3）GDCA HKMR OV CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的粤港互认机构证书；（4）GDCA HKMR IV CA，密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的粤港互认个人证书；（5）GDCA RSA ICA 密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的个人证书、机构证书、设备证书；（6）GDCA OTC CA 密钥长度为 2048-bit，签发密钥长度为 RSA 2048-bit 的个人证书、机构证书、设备证书。

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

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

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

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

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

GDCA RSA ICA 证书将在2038年12月31日到期，2036 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

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

相关的证书链信息如下：

证书链信息							
证书通用名（CN）	类型	编号（序列号）	颁发机构名称	密码算法	密钥长度	有效期	计划服务时间至
ROOTCA	根证书	69e2fec0170ac67b	NRCAC	SM3WithSM2	256 bits	2012.7.24 - 2042.7.7	
GDCA TrustAUTH E1 CA	中级CA证书（二级）	3e7e54dfdc3f77bd313bc83199218fd2	NRCAC	SM3WithSM2	256 bits	2014.6.26 - 2034.6.21	2030.1.1
GDCA SM2 ICA	中级CA证书（三级）	07000220210120010000000364631	数安时代	SM3WithSM2	256 bits	2021.1.20 - 2033.12.31	2030.1.1
GDCA Public SM2 CA1	中级CA证书（三级）	07000220210120010000000364629	数安时代	SM3WithSM2	256 bits	2021.1.20 - 2033.12.31	2030.1.1
GDCA OTC SM2 CA	中级CA证书（三级）	01f410d5d03cb50058	数安时代	SM3WithSM2	256 bits	2023.8.22 - 2033.8.22	2030.1.1
GDCA ROOT CA1	根证书	2dab67eac55ac0e4	数安时代	sha256RSA	4096 bits	2017.6.11 - 2040.12.31	2040.12.31
GDCA Public CA1	中级CA证书（二级）	275b6e832f251ca7b4d1a9b6afff925f	数安时代	sha256RSA	2048 bits	2024.7.4 - 2038.12.31	2035.1.1
GDCA Public CA2	中级CA证书（二级）	187d436e0eb2803a	数安时代	sha256RSA	2048 bits	2021.2.25 - 2038.12.31	2035.1.1
GDCA HKMR IV CA	中级CA证书（二级）	79f11a375fa55812	数安时代	sha256RSA	2048 bits	2018.9.12 - 2030.12.31	2027.1.1
GDCA HKMR OV CA	中级CA证书（二级）	2d3933c0398cde65	数安时代	sha256RSA	2048 bits	2018.9.12 - 2030.12.31	2027.1.1
GDCA RSA ICA	中级CA证书（二级）	594d645458913b3b8a1be1febc4975e2	数安时代	sha256RSA	2048 bits	2025.12.31 - 2038.12.31	2036.1.1
GDCA OTC CA	中级CA证书（二级）	4a725a2aaeca2d05	数安时代	sha256RSA	2048 bits	2018.8.22 - 2030.12.31	2028.1.1

1.3. 文档名称与标识

1.3.1 证书策略标识

本文档称作《数安时代科技股份有限公司证书策略和电子认证业务规则》（简称 GDCA CP/CPS、本 CP/CPS），CP/CPS 为“Certificate Policy and Certification Practice Statement”的缩写。在本文档中，CP/CPS 等同于本节中定义的文档名称和适用名称。GDCA 向国家 OID 注册管理中心申请了对象标识符（OID），为{1.2.156.112559}。

GDCA 遵循《TCQAE-11034-2025 电子认证业务规则规范》的证书策略 OID。

应用于粤港跨境互认的证书，同时遵循《粤港电子签名证书互认证书策略（1.1 版本）》的证书策略 OID。

1.4. 电子认证活动参与者

1.4.1. 电子认证服务机构

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》，依法设立的可信第三方电子认证服务机构。

1.4.2. 订户

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

1.4.3. 依赖方

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

1.4.4. 其他参与者

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。

1.5. 证书应用

1.5.1. 适合的证书应用

1.5.1.1. 证书签发类型

根据证书用途及应用场景，本 CP/CPS 涉及的 GDCA 签发的证书包括电子签名认证证书和非电子签名类证书。其中，电子签名认证证书包括个人电子签名认证证书、机构电子签名认证证书及粤港互认电子签名认证证书。非电子签名类证书包括加密证书、设备证书和时间戳证书。

（1） 电子签名认证证书

- 个人电子签名认证证书是为个人所签发的、用于标识个人身份的数字证书，适用于自然人或具有特定身份的人员（如公务员、企业员工等），可用于个人电子签名、数据加密应用。根据证书安全等级、身份鉴别方式等不同，个人电子签名认证证书分为个人高等级电子签名认证证书和个人基础级电子签名认证证书。
- 机构电子签名认证证书主要为政府机关、企事业单位、社会团体等所签发的、用于标识机构身份的数字证书，可用于机构电子签名、数据加密应用。根据证书安全等级、身份鉴别方式等不同，机构电子签名认证证书分为机构高等级电子签名认证证书和机构基础级电子签名认证证书。
- 粤港电子签名互认证书是为粤港跨境电子签名互认项目所签发的、用于机构和个人签名的数字证书，包括粤港互认个人电子签名认证证书和粤港互认机构电子签名认证证书，根据证书安全等级、身份鉴别方式等不同，又分为高等级和基础级电子签名认证证书。

（2） 非电子签名类证书

- 加密证书是为个人或机构签发的、用于数据加密、密钥协商等用途的数字证书，主要应用于 SM2 双证书体系场景，用于保障电子数据传输和存储过程中的机密性，不用于电子签名。
- 设备证书为各类设备（如服务器等）签发的证书，代表服务器或设备的身份，仅用于身份认证、通信通道加密等用途，不用于电子签名。

- 时间戳证书是由 GDCA 自身持有和使用、为提供可信时间戳服务而签发的数字证书，用于对时间戳响应数据进行数字签名，仅用于时间戳服务，不用于身份认证等其他用途。

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

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

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。

1.5.1.2. 各类证书的证书策略 OID 及适用性

（1） 电子签名证书

证书类型	主管部门证书策略 OID	GDCA 自定义策略 OID	密钥用法（KU）	增强型密钥用法（EKU）	适用说明
个人高等级电子签名认证证书	2.16.156.339.2.1.1.2	1.2.156.112559.1.2.1.4	digitalSignature+nonRepudiation	/	适用于高风险业务、符合《电子签名法》的个人电子签名认证证书。
个人基础级电子签名认证证书	2.16.156.339.2.1.1.1	1.2.156.112559.1.2.1.3	digitalSignature+nonRepudiation	/	适用于低风险业务、符合《电子签名法》的个人电子签名认证证书。
机构高等级电子签名认证证书	2.16.156.339.2.1.2.2	1.2.156.112559.1.2.2.2	digitalSignature+nonRepudiation	/	适用于高风险业务、符合《电子签名法》的机构电子签名认证证书。
机构基础级电子签名认证证书	2.16.156.339.2.1.2.1	1.2.156.112559.1.2.2.1	digitalSignature+nonRepudiation	/	适用于低风险业务、符合《电子签名法》的机构电子签名认证证书。
粤港互认个人高等级电子签名认证证书	2.16.156.339.2.1.1.2+2.16.156.339.1.1.1.2.1	/	digitalSignature+nonRepudiation	/	适用于高风险业务、符合《电子签名法》的个人电子签名认证证书。
粤港互认个人基础级电子签名认证证书	2.16.156.339.2.1.1.1+2.16.156.339.1.1.1.2.1	/	digitalSignature+nonRepudiation	/	适用于低风险业务、符合《电子签名法》的个人电子签名认证证书。
粤港互认机构高等级电子签名认证证书	2.16.156.339.2.1.2.2+2.16.156.339.1.1.2.2.1	/	digitalSignature+nonRepudiation	/	适用于高风险业务、符合《电子签名法》的机构电子签名认证证书。
粤港互认机构基础级电子签名认证证书	2.16.156.339.2.1.2.1+2.16.156.339.1.1.2.2.1	/	digitalSignature+nonRepudiation	/	适用于低风险业务、符合《电子签名法》的机构电子签名认证证书。

（2） 非电子签名类证书

证书类型	主管部门证书策略OID	GDCA自定义策略OID	密钥用法（KU）	增强型密钥用法（EKU）	适用说明
设备类证书	/	1.2.156.112559.1.2.3.1	digitalSignature，dataEncipherment，keyEncipherment，keyAgreement（不同场景不同组合）	id_kp_serverAuth，id_kp_clientAuth	适用于设备身份标识、通道加密，不适用于电子签名场景。
时间戳证书	/	1.2.156.112559.1.1.8.1	digitalSignature	timeStamping	用于为用户提供可信时间戳服务，对时间戳响应数据进行数字签名。
加密证书（SM2双证书）	/	/	dataEncipherment+keyEncipherment+keyAgreement		适用于采用SM2双证书体系的加密业务场景。

注：GDCA 签发的非电子签名类证书仅用于身份认证、数据加密或系统安全用途。本类证书不适用于电子签名业务，不属于《中华人民共和国电子签名法》规定的电子签名认证证书。任何单位或个人不得将本类证书作为电子签名证书使用，也不得据此主张电子签名法律效力。

1.5.2. 限制的证书应用

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

禁止在以下场景下使用 GDCA 所签发的证书，包括但不限于：

（1） 涉及人身关系，如婚姻、收养、继承等；

（2） 涉及公共事业服务停止，如停止供水、供热、供气等；

（3） 法律、行政法规规定的其他不适用电子签名的应用场景或类型；

（4） 国家法律法规禁止的活动。

涉及生命健康、财产权益等高风险活动禁止使用基础级电子签名认证证书。

1.6. 策略管理

1.6.1. 策略管理机构

GDCA 设立的安全策略委员会是 GDCA 电子认证服务所有策略的最高管理机构，负责制定、审核批准、发布、实施、更新和终止本 CP/CPS，具体职责包括但不限于：

（1） 设立 CP/CPS 编写小组，明确职能分工，建立 CP/CPS 的修订和批准流程；

（2） 对涉及信息安全策略、根证书密钥、证书签发自动审核等重要操作和流程进行审批；

（3） 每年至少进行一次 CP/CPS 的全面评审，根据监管要求变化及实际业务情况及时修订文档；

（4） 指定专门的人员形成内审和评估小组，每年针对公司的运营业务情况组织运营风险评估并形成报告。

GDCA 安全策略委员会由来自于公司管理层及业务相关部门的合适代表组成，具体成员名单以发文形式在公司范围内进行公示。安全策略委员会所有的重大会议的相关文件和会议记录由专门的部门妥善保存以备查。

1.6.2. 策略文档的批准程序

本机构的 CP/CPS 由 GDCA 安全策略委员会组织 CP/CPS 编写小组拟定文档，CP/CPS 编写小组完成后提交 GDCA 安全策略委员会审核，经该委员会批准后，正式在

GDCA 官方网站上发布，并根据《电子认证服务管理办法》的规定，从对外发布之日起的三十日之内向工业和信息化部备案。

1.7. 定义和缩写

1.7.1. 术语定义一览表

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/CPS 一致性决定机构
电子认证服务机构	取得电子认证服务许可证、为需要第三方认证的电子签名，签发电子签名认证证书并为有关各方提供真实性、可靠性验证的实体。
数字证书	也称公钥证书，由认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期及扩展信息的一种数据结构。
电子签名认证证书	由依据《中华人民共和国电子签名法》设立的电子认证服务机构签发的，可证实电子签名人与电子签名制作数据由联系的数字证书。
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。
证书策略	指明证书对于具有普通安全需求的特定团体和/或应用类的适用性的规则集合。
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。
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。
依赖方	依赖某个有效证书的自然人或法律实体。
订户	被颁发给一张证书的证书主体。
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。
高等级电子签名认证证书	适用于涉及生命健康、财产权益等高风险场景的电子签名认证证书。
基础级电子签名认证证书	适用于除高等级证书规定场景外的其他电子签名场景的证书。

1.7.2. 缩略语及其含义一览表

CA	Certification Authority	电子认证服务机构
CP/CPS	Certificate Policy and Certification Practice Statement	证书策略和电子认证业务规则
CRL	Certificate Revocation List	证书撤销列表
DN	Distinguished Name	甄别名称
GDCA	Global Digital Cybersecurity Authority CO., LTD.	数安时代科技股份有限公司
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
OID	Object Identifier	对象标识符
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)
RTO	Recovery Time Objective	恢复时间目标
RPO	Recovery Point Objective	恢复点目标

2. 信息发布与信息管理

2.1. GDCA 信息库

GDCA 信息库是一个对外公开的信息库，它能够保存、取回证书及与证书有关的信息。GDCA 信息库内容包括但不限于：

（1） CP/CPS 现行和历史版本；

（2） 证书链；

（3） 证书信息、CRL、OCSP 查询服务；

（4） 订户协议和依赖方协议；

（5） 业务办理指南，包括业务办理的流程、服务网点、营业时间、咨询电话等；

（6） 投诉处理政策及投诉方式，包括投诉电话、投诉处理部门的地址、电子邮件地址、内部监督部门名称等；

（7） 其它 GDCA 在必要时发布的信息。

GDCA 将及时发布包括证书、CP/CPS 修订和其它资料等内容，如有变化，GDCA 会在变化生效后 1 个工作日内进行更新。

2.2. 信息的发布

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。

2.3. 发布的时间和频率

GDCA 在订户证书签发或者撤销时，通过官方网站自动将证书和 CRL 发布。CRL 发布周期为 8 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。

2.4. 信息库访问控制

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。

2.5. 信息备案和对接

GDCA 严格按照国家电子认证服务管理平台的要求备案相关信息，并完成与国家电子认证服务管理平台的技术对接，实现根据证书序列号、订户身份信息等维度查询 GDCA 已签发证书列表的功能。截至本 CP/CPS 发布，国家电子认证服务管理平台相关对接要求尚未明确，GDCA 暂未开展技术对接工作。待主管部门明确相关要求后，GDCA 将按规定完成对接。

3. 身份标识与查验

3.1. 身份查验通用要求

3.1.1. 通用要求

GDCA 在受理证书申请时，按要求执行对订户和/或受托人进行告知、身份确认、意愿记录和协议签署，在完成上述流程后，才能进入证书签发环节。GDCA 自行对订户的身份进行查验，不委托给外部机构和个人（非属同一法人主体的机构视为外部机构）。

3.1.2. 订户告知

3.1.2.1.告知内容

GDCA 在订户申请证书时，明确告知以下内容：

（1）订户的权利和义务；

（2）服务收费的项目和标准；

（3）电子签名认证证书、电子签名的使用条件；

（4）信息安全保障措施；

（5）GDCA 和订户的责任划分；

（6）订户签名私钥的存储方式及安全要求；

（7）订户不得将 GDCA 签发的证书用于任何违法违规、违背公序良俗的用途，不得利用证书从事侵害国家利益、社会公共利益及第三方合法权益的活动。

3.1.2.2.告知方式

不同级别的证书其告知方式如下：

（1）高等级证书采用面对面、电话、视频或主管部门认可的其他方式告知，并保

留告知的记录。

（2）基础级证书采用高等级证书的告知方式，或采用强制阅读、短信、邮件等方式告知，并保留告知的记录。

注：采用主管部门认可的其他方式前，GDCA 应事先取得主管部门的明确认可，并在本 CP/CPS 中对相关方式及适用范围进行明确披露。

3.2. 初始身份确认

3.2.1. 证明拥有私钥的方法

订户密钥对应按本 CP/CPS 第 6.2.2 节的要求生成。

证书申请者必须证明其持有与申请证书中公钥相对应的私钥，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。

3.2.2. 个人身份的查验

对于个人证书，GDCA 必须根据个人所申请的证书级别的不同，执行不同的身份鉴别方式，证书级别越高，安全等级越高，鉴别方式越严格。如个人证书中涵盖机构信息，则需获得机构的授权。

3.2.2.1.个人身份有效性的确认

GDCA 在受理个人数字证书申请时，应对个人身份信息进行有效性查验，并按照以下要求开展核验工作：

（1）个人身份信息的提交

受理个人证书申请时，GDCA 要求订户出示其有效身份证件或提供有效身份证件信息。GDCA 认可的有效身份证件类型仅限于法律法规和国家有关文件规定的身份证件。

（2）个人身份信息有效性的查验

GDCA 应通过以下一种或多种方式查验订户身份证件的真实性和有效性：

- 通过证件机读工具对身份证件信息进行读取和核验；
- 通过权威数据库对订户身份信息进行核验；
- 通过主管部门认可的其他方式对订户身份信息进行查验。

（3）委托办理情形下的身份核验

当订户委托他人代为办理数字证书申请业务时，GDCA 应查验订户本人签署的有效书面授权证明。受托人应出示其有效身份证件或提供有效身份证件信息。GDCA 应按照本节第（2）款规定的方式，对订户和受托人的身份证件或身份资料进行有效性查验。

注：采用主管部门认可的其他方式前，GDCA 应事先取得主管部门的明确认可，并在本 CP/CPS 中对相关方式及适用范围进行明确披露。

3.2.2.2.个人高等级证书的实人查验

GDCA 采用以下方式之一完成对个人的实人查验：

（1）面对面查验；

（2）远程人工面对面查验；

（3）生物特征验证（如活体人脸、指纹、掌纹等生物识别技术的应用）；

（4）通过主管部门认可的其他方式。

在采用以上查验方式的基础上，GDCA 还可以采用认为必要的其他额外查验方式和资料。

GDCA 以可追溯的方式完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

注：采用主管部门认可的其他方式前，GDCA 应事先取得主管部门的明确认可，并在本 CP/CPS 中对相关方式及适用范围进行明确披露。

3.2.2.3.个人基础级证书的实人查验

GDCA 采用以下方式之一完成对个人的实人查验：

（1）通过第 3.2.2.2 节规定的方式；

（2）电信运营商三要素：核对姓名、证件号码、手机号在电信运营商的一致性，并通过对应手机号的随机短信验证码核验；

（3）银行卡四要素：核对姓名、证件号码、银行卡号、银行预留手机号在银行的一致性，并通过预留手机号的随机短信验证码核验；

（4）由申请人持有的有效电子签名认证证书签名验证；

（5）通过主管部门认可的其他方式，如居民身份网络可信凭证、公民网络电子身份标识、国家网络身份认证系统、内地银行或支付机构对外提供的个人账户和身份信息对应关系验证等。

在采用以上查验方式的基础上，GDCA 还可以采用认为必要的其他额外查验方式和资料。

GDCA 完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

注：采用主管部门认可的其他方式前，GDCA 应事先取得主管部门的明确认可，并在本 CP/CPS 中对相关方式及适用范围进行明确披露。

3.2.3. 机构身份的查验

对于机构证书，GDCA 必须根据机构所申请的证书级别的不同，执行不同的身份鉴别方式，证书级别越高，安全等级越高，鉴别方式越严格。

3.2.3.1.机构身份信息有效性的确认

受理机构证书申请时，GDCA 要求机构提交有效证件（如营业执照等），有效证件仅限法律法规和国家有关文件规定的证件。GDCA 通过权威第三方数据库核验机构身份的真实性和有效性。

如为法定代表人办理，GDCA 按本 CP/CPS 第 3.2.2.1.节的要求执行对法定代表人身份有效性的确认。

如为受托人办理，GDCA 按本 CP/CPS 第 3.2.2.1.节的要求执行对受托人身份有效性的确认，同时查验机构加盖公章的有效书面授权证明。

3.2.3.2.机构高等级证书的实人查验

GDCA 采用以下方式之一完成对机构的实人查验：

（1）如为法定代表人办理，GDCA 按本 CP/CPS 第 3.2.2.2.节的要求执行对法定代表人的查验。

（2）如为受托人办理，GDCA 按本 CP/CPS 第 3.2.2.2.节的要求执行对受托人的查验，并通过机构对公账户随机金额打款验证。

在采用以上查验方式的基础上，GDCA 还可以采用认为必要的其他额外查验方式和资料。

GDCA 以可追溯的方式完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

3.2.3.3.机构基础级证书的实人查验

GDCA 采用以下方式之一完成对机构的实人查验：

（1）如为法定代表人办理，GDCA 按本 CP/CPS 第 3.2.2.3.节的要求执行对法定代表人的查验。

（2）如为受托人办理，GDCA 按本 CP/CPS 第 3.2.2.3.节的要求执行对受托人的查验。

（3）由订户持有的同等级或者更高级的有效机构证书签名验证。

在采用以上查验方式的基础上，GDCA 还可以采用认为必要的其他额外查验方式和资料。

GDCA 完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

3.3. 订户意愿记录

3.3.1. 订户意愿记录内容

订户意愿记录内容，包括但不限于：

（1）订户身份信息；

（2）GDCA 的信息；

（3）签名私钥保存方及其保存义务；

（4）订户对电子签名的法律责任；

（5）订户对上述 （1）至（4）项内容已充分知晓并同意的明确意愿表示。

3.3.2. 个人高等级证书的意愿记录

GDCA 采用以下方式之一确认订户的意愿：

（1）现场办理时，通过面对面确认或手抄提示语的方式，并采用录音录像或通过主管部门认可的其他方式记录订户意愿；

（2）远程办理时，通过音视频或通过主管部门认可的其他方式确认并记录订户意愿。

注：采用主管部门认可的其他方式前，GDCA 应事先取得主管部门的明确认可，并在本 CP/CPS 中对相关方式及适用范围进行明确披露。

3.3.3. 个人基础级证书的意愿记录

GDCA 采用以下方式之一确认订户的意愿：

（1）与高等级证书相同的方式，见 3.3.2；

（2）采用强制阅读、短信或邮件进行确认等电子方式。

GDCA 保留完整、可追溯的订户意愿记录。

3.3.4. 机构高等级证书的意愿记录

GDCA 对机构高等级证书订户的申请意愿，采用以下方式之一进行确认：

（1）法定代表人申请时，GDCA 按照本 CP/CPS 第 3.3.2 节规定的方式，对机构法定代表人的意愿进行确认；

（2）受托人申请时，GDCA 查验加盖机构公章的授权文件，并按照本 CP/CPS 第 3.3.2 节规定的方式，对受托人的意愿进行确认。

GDCA 采用录音录像或主管部门认可的其他方式，对订户意愿确认过程进行记录和保存。

注：对于主管部门认可的其他记录方式，GDCA 应在实施前取得主管部门的明确认可，并在本 CP/CPS 中披露相关实现方式及适用范围。

3.3.5. 机构基础级证书的意愿记录

GDCA 对机构基础级证书订户的申请意愿，采用以下方式之一进行确认：

（1）法定代表人申请时，GDCA 按照本 CP/CPS 第 3.3.3 节规定的方式，对机构法定代表人的意愿进行确认；

（2）受托人申请时，GDCA 查验加盖机构公章的授权文件，并按照本 CP/CPS 第 3.3.3 节规定的方式，对受托人的意愿进行确认。

GDCA 保留完整、可追溯的订户意愿确认记录，并按照相关法律法规及本 CP/CPS 要求进行保存和管理。

3.4. 设备身份的鉴别

在以设备名称、IP 地址等被作为证书主题内容申请设备证书时，GDCA 应验证申请者是否拥有或控制该设备或 IP 地址的权利。确认的方式可以是提供归属权证明文件、申请者对该设备或 IP 地址所有权或使用权的书面承诺等，并加盖公章。对于证书中包含机构名称等机构身份信息的，GDCA 还应对申请机构信息的有效性进行查验，查验方式参考本 CP/CPS 第 3.2.3.1 节。

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

此外，必要时，GDCA 还可以设定其它所需要的鉴别方式和资料。

3.5. 订户协议

GDCA 的订户协议涵盖本 CP/CPS 第 3.1.2.1 中规定的内容。订户在完成上述身份查验后，在签发证书前，应按 GDCA 的要求签订订户协议，明确双方的权利、义务和责任。

3.6. 未验证的订户信息

GDCA 所签发的证书，所载明的信息都按照本 CP/CPS 第 3.1 节至第 3.4 节的查验方法、查验流程进行了验证。证书中不包含未经验证的订户信息。

3.7. 互操作要求

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 CP/CPS 必须符合 GDCA 的 CP/CPS 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。

3.8. 命名

3.8.1. 名称类型

GDCA 颁发的数字证书，含有颁发机构和证书订户主体甄别名，对证书申请者的身份和其它属性进行鉴别，并以不同的标识记录其信息。证书持有者的标识命名，以甄别名（Distinguished Name）形式包含在证书主体内，是证书持有者的唯一识别名。GDCA 的证书符合 X.509 标准，分配给证书持有者实体的甄别名，采用 X.500 标准命名方式。DN 项结构定义符合 GB/T 16264.8 的要求。

GDCA 证书颁发机构的主体甄别名命名规则如下：

属性	值
国家（C）	CN
省（S）	证书颁发者所在省份（可选）
地区（L）	证书颁发者所在城市（可选）
机构（O）	Global Digital Cybersecurity Authority Co., Ltd.或

	GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.
机构部门（OU）	GDCA 可能依据用户类型、应用领域、区域的不同采用不同的颁发者为用户颁发证书，所以 GDCA 证书中可以包含不同的颁发者名称。
通用名（CN）	此属性为 CA 名

GDCA 证书订户的主体甄别名命名规则如下：

属性	值
国家（C）	CN
省（S）	省份（可选）
地区（L）	城市（可选）
机构（O）	订户所在机构信息（可选）
机构部门（OU）	订户所在机构的部门信息（可选）
通用名（CN）	订户名称（个人姓名或机构法定名称或设备名称）

GDCA 根据证书类型的不同，采用不同的 DN 命名规则。

（1）个人证书命名规则

个人证书主体 DN 中的 CN 项应填写订户本人真实姓名，并应与订户提交的有效身份证明文件中的姓名保持一致。GDCA 将在证书 DN 项或扩展项中包含订户有效身份证件类型及其编号，或包含对应身份信息的映射值（包括但不限于散列值、掩码等），以确保主体身份可追溯至唯一自然人。对于需要体现订户所属机构信息的个人证书，可在 O 项中填写机构名称，如填写机构名称，应与订户提交的有效主体身份证明文件中的名称保持一致。个人证书 DN 示例如下：

C=CN，S=广东省，L=广州市，CN=张三

或者：

C=CN，S=广东省，L=广州市，O=XX 有限公司，CN=张三

（2）机构证书命名规则

机构证书主体 DN 中的 O 项及 CN 项应包含机构名称，并与订户提交的有效主体身份证明文件中的名称保持一致。GDCA 将在证书 DN 项或扩展项中包含机构有效身份证件类型及其编号，以确保主体身份可追溯至唯一机构实体。

机构证书 DN 示例如下：

C=CN，S=广东省，L=广州市，O=XX 有限公司，CN=XX 有限公司

如机构存在部门信息，可在 OU 项中填写机构部门名称。

（3）设备证书命名规则

设备证书主体 DN 中的 CN 项应包含设备名称、设备编号或者其他能够标识设备的信息。设备所属机构名称可根据业务场景填写在 O 项中，如填写，应与订户提交的有效主体身份证明文件中的名称保持一致。

设备证书 DN 示例如下：

C=CN，CN=XX（设备信息）

或者：

C=CN，O=XX 有限公司，CN= XX（设备信息）

3.8.2. 对名称意义化的要求

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

对于个人证书，主体 DN 项中包含订户姓名，在 DN 项或扩展项中包含有效证件类型及其编号（或相关信息的映射，包括但不限于散列值、掩码等）。

对于机构证书，主体 DN 项中包含机构名称，在 DN 项或扩展项中包含组织机构的有效证件类型及其编号。

3.8.3. 订户的匿名或伪名

本 CP/CPS 规定，GDCA 的订户在进行数字证书申请时不能使用匿名或伪名。

3.8.4. 理解不同名称的形式的规则

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

3.8.5. 名称的唯一性

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

3.8.6. 商标的识别、鉴别与角色

GDCA 签发数字证书时，以经核验的自然人姓名、机构法定名称、设备名称或其他经验证的主体标识作为证书主体甄别名称，不以商标名称作为独立身份标识进行证书命名。当订户法定名称中包含注册商标、字号、品牌名称或其他商业标识时，GDCA 依据订户提交的有效身份证明文件进行核验，并按照经核验的主体名称进行证书签发。

订户应保证其申请使用的名称、商标、字号、品牌名称及其他标识具有合法使用权，并承担由此产生的法律责任。对于存在明显侵权风险、可能导致公众混淆误认、涉嫌冒用他人合法权益或者收到相关权利人异议的情形，GDCA 有权要求订户补充证明材料、拒绝签发或者撤销相关证书。

4. 证书生存周期操作要求

4.1. 通用要求

GDCA 在证书申请、身份鉴别、证书签发、证书管理及相关服务过程中，明确各参与方的责任和义务。包括但不限于：

（1）GDCA 有建立、运营和维护注册通道的责任。

（2）GDCA 承担与订户签订电子认证服务协议的责任。

（3）GDCA 承担对订户提供的证书申请信息与身份证明资料的一致性检查工作，妥善记录并保存证书生存周期过程中所涉及的相关信息。

（4）订户承担向 GDCA 提供真实、完整和准确的证书申请信息和资料的责任。

4.2. 证书申请

4.2.1. 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(包括国家机关、事业单位、社会团体和人民团体等)。

4.2.2. 注册过程

证书注册过程包括以下关键环节：

（1）订户向 GDCA 提交证书申请及相关申请资料。

（2）GDCA 按照证书类型和等级要求，对订户身份、申请信息以及相关证明材料进行审核和验证。

（3）审核通过后，GDCA 按照内部流程完成证书签发。

（4）GDCA 向订户签发数字证书，并通过安全可靠的方式完成证书交付。

（5）GDCA 对证书注册过程中形成的申请资料、审核记录、身份鉴别记录、签发记录及交付记录进行保存和管理。

4.2.3. 证书申请处理

（1）识别与鉴别功能

当 GDCA 接受到订户的证书申请后，应按本 CP/CPS 第 3 章的要求，完成对订户的告知、身份确认、意愿记录、协议签署等环节，通过有效手段确保证书信息的真实性和有效性，并将证书签发给正确的申请者。

（2）证书申请的批准

GDCA 成功完成了证书申请所有必需的确认步骤并提交证书请求后，GDCA 通过颁发正式证书来批准证书申请。 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/CPS 第 3 章关于订户身份的标识和查验的规定；

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。

（3）证书申请的拒绝

如果发生下列情形，GDCA 拒绝证书申请：

1） 该申请不符合本 CP/CPS 第 3 章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） GDCA 认为批准该申请将会对 GDCA 带来争议、法律纠纷或者损失。

6） 对于拒绝的证书申请，GDCA 通知申请者证书申请失败。

4.2.4. 处理证书申请的时间

GDCA 在受理订户证书申请后，将及时开展身份鉴别、申请信息审核及证书签发工作。在订户提交完整、真实、准确且符合要求的申请资料，并完成身份鉴别所需流程的情况下，GDCA 原则上自受理之日起 5 个工作日内完成证书申请处理，包括完成审核并作出签发或者拒绝签发决定。

对于因申请资料存在问题、需要补充证明材料、需要进一步核实身份信息、不可抗力或其他特殊原因导致无法在上述期限内完成处理的，GDCA 将及时告知订户相关情况，

并与订户协商确定后续处理时限。

证书申请处理时限的实现取决于订户是否及时、真实、准确、完整地提交申请资料，以及是否及时配合 GDCA 完成身份鉴别和信息核验工作。

4.3. 证书签发

4.3.1. 证书签发过程中认证服务机构的行为

GDCA 在完成订户身份鉴别、申请信息审核及相关验证工作后，根据审核结果决定是否签发数字证书。

对于审核通过的证书申请，GDCA 按照本 CP/CPS 及相关技术规范要求生成证书内容，并完成证书签发。证书签发意味着 GDCA 已完成对证书申请的审核，并正式批准该证书申请。对于审核未通过或者不符合证书签发条件的申请，GDCA 有权拒绝签发证书，并根据实际情况要求订户补充相关证明材料或者重新提交申请。

4.3.2. 电子认证服务机构和注册机构对订户的通告

GDCA 在完成证书申请处理后，将以一种或多种适当方式向订户通告处理结果。通告方式包括但不限于：

（1）通过证书申请系统、认证应用工具、业务办理平台或其他渠道进行信息提示；

（2）通过信函、电子邮件、站内信、系统消息等电子方式发送通知；

（3）通过短信方式发送通知；

（4）通过电话方式通知；

（5）通过当面告知、实时视频等相当于面对面的方式通知；

（6）通过主管部门认可的其他方式通知。

4.4. 证书接受

4.4.1. 构成接受证书的行为

订户应在收到数字证书后及时核验证书内容是否与申请信息一致。发生下列情形之一的，视为订户已接受证书：

（1）订户自行通过 GDCA 提供的证书服务系统、工具或其他服务渠道下载并获取数字证书；

（2）GDCA 按照订户要求将数字证书写入数字证书载体或其他安全介质并交付订户，订户领取或接收相关载体；

（3）订户激活、安装、部署或启用数字证书；

（4）订户使用数字证书进行电子签名、数据加密或其他证书应用操作；

（5）其他能够证明订户接受数字证书的行为。

订户发现证书信息与申请信息不一致、证书内容存在错误或者其他异常情况时，应及时向 GDCA 提出异议。GDCA 将根据实际情况进行核查和处理。

GDCA 保存订户接受证书的相关记录，包括但不限于接受时间、接受方式、相关操作人及操作记录及其他能够证明订户接受证书的证据材料。

4.4.2. 电子认证服务机构对证书的发布

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

4.4.3. 电子认证服务机构对其他实体的通告

除法律法规、主管部门要求或者本 CP/CPS 另有规定外，GDCA 不单独向其他实体通告证书签发结果。依赖方及其他相关实体可通过 GDCA 提供的证书目录服务、证书状态查询服务获取相关证书信息。

4.5. 密钥对和证书的使用

4.5.1. 订户的私钥和证书的使用

4.5.1.1 订户自行保管签名私钥

对于由订户自行保管签名私钥的应用场景，订户应按照本 CP/CPS、电子认证服务协议及相关法律法规要求使用其数字证书，并采取合理措施妥善保管其签名私钥、证书载体及口令息，防止私钥泄露、丢失、被盗用、被篡改或者被未经授权使用。在将密钥对交付订户保管之前，GDCA 采取必要的技术和管理措施保障密钥对的安全性，包括但不限于：

（1）保障签名私钥生成和传输过程的安全；

（2）对订户提交或者生成的公钥进行安全性检查，并依据国家标准、行业规范及本 CPS 要求审核密钥算法和密钥长度；

（3）对于不符合国家或者行业安全标准要求的密钥或者算法，GDCA 有权拒绝签发证书，包括但不限于 RSA 密钥长度小于 2048 位、使用 MD5、SHA-1 等已被

证明存在安全风险或者不再符合行业安全要求的密码算法。

对于由订户自行保管签名私钥的应用场景，GDCA 不保存订户签名私钥。

4.5.1.2 GDCA 提供签名私钥管理服务

对于云签名、远程签名等由 GDCA 提供签名私钥管理服务的应用场景，GDCA 按照国家法律法规及相关技术标准要求，对订户签名私钥实施安全管理。GDCA 提供签名私钥管理服务时，应采取必要的管理和技术措施保障签名私钥安全，并遵守以下要求：

（1）在保存订户签名私钥之前，应取得订户书面授权；

（2）未经订户书面授权，不得保存或者委托他人保存订户签名私钥；

（3）机构证书签名私钥的使用，应由法定代表人或者其合法授权代表进行授权；

（4）仅在获得订户明确授权的情况下使用订户签名私钥完成电子签名操作；

（5）签名私钥应以加密形式存储，且存储条件符合安全标准；

（6）所有涉及签名私钥生成、存储、授权、使用、变更和销毁等操作均应保留完整、可追溯的记录。

4.5.2. 安全事件反馈

订户、依赖方等如发现证书信息错误、私钥失密或证书被盗用等异常情况，可通过以下途径进行反馈：

电子邮箱：gdca@gdca.com.cn

电话号码：4007008088

4.6. 证书续期

证书续期指在不改变证书订户的公钥或其他任何信息的情况下，在原证书到期前，为订户签发一张新证书。

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

4.6.1. 证书续期的情形

对于 GDCA 签发给订户的证书，订户需在证书到期前进行证书续期。

当订户证书即将到期且主体身份信息未发生变化时，可以向 GDCA 申请证书续期。

如订户身份信息、证书主体信息发生变化，则不适用证书续期，应按照新证书申请流程重新办理。

4.6.2. 请求证书续期的实体

请求证书续期的实体为证书订户或其受托人。

4.6.3. 证书续期请求的处理

GDCA 在处理证书续期申请时，应对申请人身份进行确认。

自申请人上次完成身份查验之日起至本次续期申请日未满三年的，GDCA 可以通过验证有效原证书电子签名的方式确认申请人身份。

自申请人上次完成身份查验之日起至本次续期申请日已满三年的，GDCA 应按照本 CPS 第 3.2 节规定重新开展身份查验。GDCA 在任何情况下都可将这种初始证书申请的鉴别方式作为证书更新时的鉴别处理手段。

对于身份信息发生变化、存在安全风险或者 GDCA 认为有必要重新核验身份的情形，GDCA 有权要求申请人重新完成身份查验。

续期证书的签发流程应符合本 CP/CPS 第 4.3 节的规定。

4.6.4. 颁发新证书时对订户的通告

同本 CP/CPS 第 4.3.2 节。

4.6.5. 构成接受续期证书的行为

同本 CP/CPS 第 4.4.1 节。

4.6.6. 电子认证服务机构对续期证书的发布

同本 CP/CPS 第 4.4.2 节。

4.6.7. 电子认证服务机构对其他实体的通告

同本 CP/CPS 第 4.4.3 节。

4.7. 证书密钥更新

证书密钥更新指为订户生成新的密钥对并为其新公钥签发新证书。

4.7.1. 证书密钥更新的情形

出现以下情形之一时，订户可以向 GDCA 申请证书密钥更新：

（1）原证书对应密钥对即将达到使用期限；

（2）订户认为原密钥存在安全风险；

（3）原证书私钥泄露而撤销证书；

（4）法律法规、行业标准或者主管部门要求进行密钥更新。

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或其受托人。

4.7.3. 证书密钥更新请求的处理

GDCA 在处理证书密钥更新申请时，应对申请人身份进行确认。

自申请人上次完成身份查验之日起至本次密钥更新申请日未满三年的，GDCA 可以通过验证有效原证书电子签名的方式确认申请人身份。

自申请人上次完成身份查验之日起至本次密钥更新申请日已满三年的，或存在本 CP/CPS 第 4.7.1 节第（2）、（3）种情形，或者其他导致原证书对应密钥存在安全风险、不再适合作为申请人身份确认依据的情形，GDCA 应按照本 CP/CPS 第 3.2 节规定重新开展身份查验。

对于身份信息发生变化密钥存在安全风险或者 GDCA 认为有必要重新核验身份的情形，GDCA 有权要求申请人重新完成身份查验。

密钥更新的证书签发流程应符合本 CP/CPS 第 4.3 节的规定。

4.7.4. 颁发新证书时对订户的通告

同本 CP/CPS 第 4.3.2 节。

4.7.5. 构成接受密钥更新证书的行为

同本 CP/CPS 第 4.4.1 节。

4.7.6. 电子认证服务机构对密钥更新证书的发布

同本 CP/CPS 第 4.4.2 节。

4.7.7. 电子认证服务机构对其他实体的通告

同本 CP/CPS 第 4.4.3 节。

4.8. 证书变更

证书变更是指改变证书中除订户公钥之外的信息而签发新证书的情形。证书信息发

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

4.8.1. 证书变更的情形

出现以下情形之一时，订户可以申请证书变更：

（1）订户名称发生变更；

（2）订户身份证件或者机构身份证明信息发生变更；

（3）证书中载明的其他主体信息发生变更；

（4）法律法规、行业标准或者主管部门要求变更证书信息的其他情形。

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或其受托人。

4.8.3. 证书变更请求的处理

证书变更按照初次申请证书的注册过程进行处理。GDCA 在处理证书变更申请时，按照本 CP/CPS 第 3.2 节规定对申请人身份信息进行查验和确认。

变更证书的签发流程应符合本 CP/CPS 第 4.3 节的规定。

4.8.4. 颁发新证书时对订户的通告

同本 CP/CPS 第 4.3.2 节。

4.8.5. 构成接受变更证书的行为

同本 CP/CPS 第 4.4.1 节。

4.8.6. 电子认证服务机构对变更证书的发布

同本 CP/CPS 第 4.4.2 节。

4.8.7. 电子认证服务机构对其他实体的通告

同本 CP/CPS 第 4.4.3 节。

4.9. 证书撤销或冻结

4.9.1. 证书撤销的情形

当数字证书的可信性、安全性或者有效性受到影响，订户可以申请撤销证书，GDCA 也可以根据法律法规、本 CP/CPS 规定或者风险管理需要主动撤销证书。

（一）订户申请撤销

出现下列情形之一的，订户可以向 GDCA 申请撤销证书：

（1）订户发现证书对应私钥已经遗失、泄露、被盗用；

（2）订户确认最初证书申请未经授权且无法追溯至合法授权行为；

（3）订户身份信息或者证书信息发生重大变化，不再适合继续使用原证书；

（4）其他需要撤销证书的情形。

（二）GDCA 主动撤销

若出现以下情况中的一种或多种，GDCA 有权撤销证书：

（1）GDCA 获得了证据，证明与证书公钥对应的订户私钥遭到了泄漏。

（2）GDCA 获得证据证明证书被用于非法用途、超出证书规定用途使用或者存在其他误用情形；

（3）GDCA 发现订户提交虚假材料、提供错误信息或者隐瞒重要事实；

（4）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；

（5）GDCA 获悉证书中所含信息出现重大变化；

（6）GDCA 认为任何或被告知出现在证书中的信息为错误信息；

（7）因不可抗力、重大安全事件、系统安全风险或者其他原因导致证书继续有效可能影响电子认证服务安全运行；

（8）GDCA 已经履行催缴义务后，订户仍未缴纳服务费；

（9）法律法规、主管部门要求撤销证书。

4.9.2. 请求证书撤销的实体

请求证书撤销实体为订户、受托人、GDCA、依赖方、依法履行职责的司法机关授权人员。

4.9.3. 撤销请求的流程

GDCA 提供热线电话等便捷渠道，记录影响证书或私钥安全的事件，包括但不限

于密钥遗失、泄露及证书被盗用或冒用等。安全事件的反馈及便捷渠道同本 CP/CPS 第 4.5.2 节。GDCA 在完成身份验证和申请审核后，根据审核结果作出撤销或者不予受理的决定，并通知申请人。

4.9.3.1. 订户主动提出撤销申请

订户或者其合法授权的受托人可以通过 GDCA 公布的热线电话、在线服务平台、或者其他认可方式提出证书撤销申请。

GDCA 在受理撤销申请时，应核验申请人的身份及申请权限。必要时，GDCA 有权要求申请人提供身份证明文件、授权文件或者其他证明材料。

经核验符合受理条件的，GDCA 应按照内部审批流程完成证书撤销处理。GDCA 原则上应自受理撤销申请之时起 24 小时内完成证书撤销操作。

4.9.3.2. GDCA 主动撤销证书

当出现本 CP/CPS 第 4.9.1.1 节规定的证书撤销情形时，GDCA 有权主动撤销相关证书。GDCA 在作出撤销决定前，应根据具体情况核实相关事实和证据。对于涉及私钥泄露、证书误签发、身份信息失实或者其他重大安全风险的情形，GDCA 可以启动紧急处置程序并直接实施证书撤销。

证书撤销后，GDCA 应通过适当方式通知订户，包括但不限于电子邮件、短信、电话、业务系统站内消息或者其他有效方式，并告知证书撤销的原因。

因联系方式失效、无法取得联系或者其他客观原因导致无法通知订户的，GDCA 可以通过官方网站或者其他适当方式发布相关公告。

4.9.3.3. 电子认证服务机构本身证书的撤销

对于GDCA运营和管理的根证书、中级CA证书以及其他用于电子认证服务的证书，GDCA 应依据本 CP/CPS、相关管理制度、主管部门要求以及风险管理需要决定是否实施证书撤销。

GDCA 应建立 CA 证书撤销审批机制，并保存证书撤销申请、审批、执行、及相关处理过程记录。

4.9.4. 撤销请求宽限期

订户或者其他有权申请撤销证书的实体发现或者怀疑存在影响证书可信性、安全性或者有效性的情形时，应及时向 GDCA 提出证书撤销申请，撤销申请便捷渠道见本

CP/CPS 第 4.5.2 节。对于私钥遗失、泄露、被盗用等重大安全事件，申请人应在发现相关情况后 24 小时内通知 GDCA。

GDCA 收到撤销申请后，应按照本 CP/CPS 规定及时完成处理。

4.9.5. 电子认证服务机构处理撤销请求的时限

GDCA 在受理证书撤销申请后，应及时完成相关核验和处理工作。对于符合受理条件的撤销申请，GDCA 原则上应在 24 小时内完成证书撤销操作。

4.9.6. 依赖方检查证书撤销的要求

依赖方在信赖数字证书前，应对证书状态进行验证。

GDCA 向订户和依赖方提供证书状态查询服务，包括证书撤销列表（CRL）服务、在线证书状态协议（OCSP）服务。

依赖方应通过 CRL 或 OCSP 方式查询证书状态，并结合证书有效期、证书路径验证结果等信息综合判断证书的可信状态。

4.9.7. CRL 发布频率

GDCA 对证书吊销列表（CRL）的发布机制如下：

（1）订户证书 CRL

GDCA 对所签发的订户证书 CRL 进行定期更新，更新间隔不超过 8 小时，即 CRL 的本次发布与下一次发布之间的最大时间间隔不超过 8 小时。

（2）中级 CA 证书 CRL

对于中级 CA 证书， CRL 的最大更新间隔不超过 12 个月。在发生中级 CA 证书撤销的情况下，GDCA 将在撤销操作完成后 24 小时内发布更新后的 CRL。

（3）紧急 CRL 更新机制

在发生重大安全事件或其他紧急情况下，GDCA 可启动紧急 CRL 更新机制，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。

4.9.8. CRL 发布的最大滞后时间

GDCA 确保 CRL 在既定发布周期到期后，最迟不超过 24 小时完成新 CRL 的生成与发布。

4.9.9. 在线状态查询的可用性

GDCA 向证书订户和依赖方提供在线证书状态查询服务。OCSP 响应须符合 RFC6960 的要求，并且被 OCSP 响应签名密钥进行数字签名。

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，GDCA 不对合法查询设置访问权限限制。

4.9.11.撤销信息的其他发布形式

GDCA 不提供撤销信息的其他发布形式。

4.9.12.密钥损害的特别要求

除本 CP/CPS 第 4.9.1 节规定的情形外，当订户证书密钥已经失密或者可能已经失密时，订户必须及时向 GDCA 提出证书撤销请求。

4.9.13.证书冻结的情形

不适用。

4.9.14.请求证书冻结的实体

不适用。

4.9.15.冻结请求的流程

不适用。

4.9.16.冻结的期限限制

不适用。

4.10.证书状态信息服务

4.10.1.证书信息状态服务方式

GDCA 通过证书吊销列表（CRL）和在线证书状态协议（OCSP）向订户、依赖方及其他相关方提供证书状态信息查询服务。GDCA 定期发布并更新 CRL，供相关方下载查询证书状态，同时提供 OCSP 在线查询服务，为相关方提供证书状态实时查询能力。

GDCA 应确保上述证书状态信息服务具备与业务规模相适应的响应能力和并发处

理能力。

4.10.2.证书状态信息服务

GDCA 提供 7*24 小时连续不间断的证书状态查询服务，包括 CRL 发布服务和 OCSP 在线查询服务。在正常运行情况下，证书状态信息查询服务响应时间不超过 10 秒。

证书状态信息查询服务年度可用率不低于 99%。在网络通信正常且系统运行正常的情况下，相关方可通过 GDCA 提供的查询渠道及时获取证书状态信息。

4.10.3.备用查询机制

GDCA 提供 CRL 和 OCSP 两种证书状态信息服务方式。当 OCSP 在线查询服务不可用时，订户、依赖方及其他相关方可通过 GDCA 公布的 CRL 发布地址获取最新证书吊销列表（CRL），查询证书状态信息。

4.11.停止使用认证服务

4.11.1.停止使用认证服务的情形

订户停止使用 GDCA 提供的电子认证服务包括以下情形：

（1）订户主动申请停止使用电子认证服务；

（2）订户申请撤销数字证书且 GDCA 完成证书撤销处理；

（3）证书有效期届满后，订户未申请证书续期或密钥更新；

（4）法律法规、监管要求或主管部门要求停止提供电子认证服务的其他情形。

4.11.2.停止服务请求的处理时限和方式

订户申请停止使用电子认证服务的，应按照本 CP/CPS 第 4.9.3 节规定提交申请。GDCA 应按照本 CP/CPS 第 4.9.5 节规定的时限完成处理。

GDCA 批准停止服务申请后，应根据业务类型采取相应措施，包括但不限于：

（1）撤销相关数字证书；

（2）通过 CRL、OCSP 等证书状态信息服务发布证书状态变更信息；

（3）对于由 GDCA 生成、托管或管理订户签名私钥的应用场景，按照密钥管理要求对相关私钥进行安全销毁并保留记录；

（4）对于由订户自行生成和保管私钥的业务场景，GDCA 应提示订户停止使用相关私钥。

4.11.3.用户数据的保存、销毁与转移

停止服务后，GDCA 应按照本 CP/CPS 及相关管理制度保存用户申请资料、身份鉴别记录、证书签发记录及相关日志信息。

保存期限届满后，GDCA 应按照信息安全管理要求对相关数据进行安全销毁。法律法规、监管要求另有规定的，从其规定。

因法律法规、监管要求、业务迁移或其他合法原因需要转移相关数据的，GDCA 应采取必要措施保障数据的完整性、真实性和机密性。

4.11.4.停止服务后的责任延续

停止提供电子认证服务后，不影响服务终止前已经签发证书、完成电子签名或者形成电子认证活动所产生的法律效力。GDCA、订户及依赖方在服务终止前已经产生的权利、义务和责任，不因服务终止而免除。

4.11.5.操作记录

GDCA 应完整记录停止服务申请、审核审批、证书撤销、密钥销毁（如适用）、数据处理及归档等操作过程，并按照本 CP/CPS 第 5 章的相关要求保存记录。

4.12.密钥托管与恢复

GDCA 的根证书私钥在主机房核心区生成并存储，使用经国家密码主管部门批准的密码设备进行保护与管理。根证书私钥不托管给任何第三方机构或个人。

GDCA 建立了根证书密钥备份与恢复策略，对根证书密钥进行安全备份管理。

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

GDCA 的建筑物和机房建设按照下列标准实施：

- GB/T25056-2018《信息安全技术 证书认证系统密码及其相关安全技术规范》
- GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》
- GB50174-2017《数据中心设计规范》
- GB/T36340-2018《防静电活动地板通用规范》

- GB/T2887-2011《计算机场地通用规范》
- GB50462-2024《数据中心基础设施施工及验收标准》
- GB50222-2017《建筑内部装修设计防火规范》
- GB50116-2013《火灾自动报警系统设计规范》
- GB50057-2010《建筑物防雷设计规范》
- GB50054-2011《低压配电设计规范》
- GB50019-2015《工业建筑供暖通风与空气调节设计规范》

GDCA 机房位于佛山市南海区狮山镇，是一幢独立的建筑物，具备防震、防火、防水、防雷等功能，进入机房建筑区只有唯一的入口和道路，GDCA 中心机房按照功能主要分为核心区、服务区、管理区、操作区、公共区五个区域。只有经过授权的人员才能进入授权的区域。

5.1.1.1. 公共区域

公共区包括入口、大堂、保安室，部署各配套设施和监控设备。

5.1.1.2. 操作区

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

5.1.1.3. 管理区

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

5.1.1.4. 服务区

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

5.1.1.5. 核心区

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

核心区，存放保密资料。

5.1.2. 物理访问

GDCA 机房内设有 8 扇门安装电子门禁系统和 1 个物理侵入报警器，对门禁系统进行监控，实时读取门禁记录的资料，并对门禁系统设置权限。该系统能实时读取进出门资料，并有门开超时报警。工作人员都需使用身份识别卡或结合指纹才能进出，并且进出每一道门都有时间记录和相关信息提示，服务区与核心区需要两个管理员同时使用身份识别卡和指纹鉴别才可以进入，机房工作人员按照机房日常工作规范，每月对门禁记录进行整理归档，保留一年的门禁记录。

物理访问控制包括如下几个方面：

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

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

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

5.1.3. 安防监控

根据机房动力环境保安监控系统的要求，本机房环境监控系统包括的子系统有：配电检测子系统、UPS 检测子系统、空调设备检测子系统、新风机检测子系统、温湿度检测子系统、漏水监测子系统、消防子系统、门禁子系统、图像监控子系统。对基础设施设备、机房环境状况、安防系统状况进行 7*24 小时实时监测，为满足故障诊断、事后审计的需要，监控记录保留时间为 6 个月以上。其中非公共区域（服务区、管理区、核心区）的监控记录在销毁前进行安全审计，形成的审计报告存档备查。

5.1.4. 电力与空调

本机房采用高压环网供电体系，配置柴油发电机组及双路 UPS 不间断供电系统，构建多层级闭环冗余供电架构，全方位保障电力持续稳定输出；在市电中断工况下，可实现 12 小时以上不间断应急供电。配置有专门的配电房，每个机房配置有独立的配电设备、接地防雷系统。机房区域内采用了防静电措施，实现机柜、服务器、网络设备等电位连接和接地。

机房的空调采用风冷式冷凝器机组。机房按照 300kcal/h ㎡ 热负荷计算。夏季室外设计温度：35℃；冬季室外设计温度：0℃；机房室内设计温度：22±1℃，相对湿度：55±5%/h 。同时，机房安置了新风系统，对机房进行换气，保证机房内的空气品质和解决新风供应以及机房对空气清洁度的要求等问题。

5.1.5. 水患防治

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

5.1.6. 火灾防护

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

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

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

当自动、手动紧急启动都失灵时，可进入储瓶间内实现机械应急操作启动。

5.1.7. 存储媒体管理

GDCA 对物理介质的存放和使用满足防火、防水、防震、防潮、防腐蚀、防虫害、防静电、防电磁辐射等的安全需求。采取了介质使用登记注册、介质防复制及信息加密等措施实现了对介质的安全保护。

GDCA 对存储媒体使用、报废管理有具体的规定，包括使用权限、报废标准、销毁方法和审批流程，完整记录存储媒体领用、归还、报废等情况。

5.1.8. 设备管理

建立了设备台账，设备台账包含每台设备的责任人、使用状态、维护周期和报废标准；定期对设备进行盘点和核对，确保设备实际情况与设备台账相符。

5.1.9. 废物处理

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。

5.1.10. 异地备份

GDCA 在距离主机房直线距离 25km 处的佛山市办公场地三山科创中心建立了异地数据备份中心，对关键系统数据和其他重要信息进行异地备份。

5.2. 操作过程控制

5.2.1. 可信角色

在 GDCA 提供的电子认证服务过程中，所有对 GDCA 证书认证系统的操作、维护、管理及核心业务有访问权限或重要影响的职位都被 GDCA 视为可信角色。可信角色需通过严格的身份验证、授权审批及权限分离控制，并遵循最小权限与职责分离原则。GDCA 定义的可信角色包括但不限于以下类型：

（1）系统管理员：负责系统安全策略配置、可信角色系统账户与权限管理等。

（2）技术运维员：负责物理环境、网络、服务器及系统软件的日常监控与维护等。

（3）数据库管理员：负责数据库进行日常运维、性能优化及数据备份等。

（4）系统审计员：负责系统和网络日志的审计、管理、审计报告生成等。

（5）密钥管理员：负责根证书私钥的生成、备份、存储、恢复、归档和销毁的全生存周期管理，硬件安全模块的管理等，执行多因子控制（M of N），使用智能卡和密码访问，确保多因子控制机制的有效运行和备份。

（6）业务操作员：负责证书申请的受理、审核，订户的身份与意愿鉴证，使用证书和密码登录，受理和审核分开，初审和复核分离。

（7）客户档案管理员：负责客户证书相关档案资料的归档与保密等。

（8）运营审计员：负责对客户签发、客户服务等核心业务进行独立审计等。

（9）其他人员：对公司运营有重要影响的其他管理人员。

5.2.2. 职责分离

GDCA 遵循职责分离原则，所有涉及关键操作（密钥管理、审计、鉴证、系统管理）的角色应实现双人操作或复核机制；涉及业务连续性相关的操作（运维、鉴证、审计等）的角色按工作量设置人员冗余，在任何一人缺岗时仍能实现双人操作；同一人员不得掌握可独立完成“发起、审批、执行、审计”全流程的任何组合。下列角色不得相关兼任：

（1）系统管理员、技术运维员、数据库管理员、系统审计员之间不得兼任；

（2）同一证书业务的录入与审核环节不得由同一业务操作员完成；

（3）业务操作员、客户档案管理员、运营审计员之间不得兼任；

（4）密钥管理员不得与系统管理员、技术运维员兼任；

（5）密钥管理员不宜与除策略管理机构成员外的其他可信角色兼任。

5.3. 人员控制

5.3.1. 可信人员资格要求

GDCA 对承担可信角色的工作人员的资格、经历和背景等进行调查，要求如下：

（1）背景调查要求

GDCA 在人员录用、岗位调整或授权前，对拟担任可信角色的人员开展必要的背景调查及核验，包括教育经历、工作经历及职业诚信等方面的审查。可信角色人员应无与岗位职责不相适应的不良从业记录，并按要求完成无犯罪记录等相关审查。

（2）专业技能要求

可信角色人员应具备履行岗位职责所需的专业知识、技能和工作经验，熟悉电子认证服务相关法律法规、标准规范、安全管理制度及岗位操作规程。涉及系统管理、密钥管理、审计、身份鉴别等关键岗位的人员应接受相应培训并具备岗位所需的专业能力。

（3）保密义务要求

可信角色人员应签署具有法律约束力的保密协议，承诺遵守 GDCA 信息安全和保密管理相关制度，不得以任何方式私自保存、复制、传播、披露或向未经授权的人员提供电子认证服务相关的秘密信息、敏感信息及其他受保护信息。

（4）劳动关系要求

可信角色人员应与 GDCA 依法建立劳动关系并签署劳动合同，在获得岗位授权前应明确岗位职责、安全责任等要求。

5.3.2. 可信人员培训要求

GDCA 建立覆盖所有可信角色的持续培训体系，确保相关人员具备履行岗位职责所需的专业知识、业务能力和安全合规意识。

（1）岗前培训

所有拟担任可信角色的人员，在获得岗位授权前应完成岗前培训并通过考核。岗前培训时长不少于 20 学时，培训内容应覆盖岗位职责、电子认证服务相关法律法规及岗位操作规范等内容。未经培训或考核不合格的人员不得从事相关岗位工作。

（2）持续培训

GDCA 对可信角色人员实施持续培训管理。所有可信角色人员每年至少接受一次培训，每人每年累计培训时长不少于 20 学时，并应通过相应考核。培训记录、考核结果及相关证明材料应妥善保存。

（3）培训内容

可信角色培训内容至少包括：

- 电子认证服务相关法律法规与标准；
- 岗位通用职责要求及各角色特定的工作要求；
- GDCA 内部管理政策、制度及流程等；
- PKI 体系及密码技术基础知识；
- 证书策略和电子认证业务规则（CP/CPS）；
- 安全管理策略和机制；
- 订户身份查验和审核策略和流程；
- 电子认证服务运营体系构成；
- 电子认证服务技术体系构成；
- 灾难恢复和业务连续性管理。

5.4. 审计日志程序

5.4.1. 记录事件的内容及范围

GDCA 建立覆盖电子认证服务全生命周期的审计日志管理机制，对系统运行、证书生命周期管理、密钥管理、安全事件及物理环境管理等活动进行持续、完整的记录，并定期开展日志审计。

（1）审计日志记录范围

GDCA 持续记录与电子认证服务相关的关键操作和安全事件，包括但不限于：

1）根证书密钥操作：包括密钥生成、备份、存储、恢复、归档、销毁，以及密码设备的启用、停用、转移和销毁等；

2）系统访问行为：包括所有对系统的访问企图，包括成功的和失败的登录、退出、权限使用行为等；

3）系统操作与变更：包括对系统的各种关键查询、修改、删除等操作，系统组件的安装、升级、维修，人员，以及敏感信息的获取与取阅等；

4）网络安全事件：包括防火墙、路由器、入侵检测安全设备记录的告警信息，以及针对被攻击事件识别与相应处理过程、结果等；

5）证书生存周期关键过程:包括记录证书申请、审核、发、更新、变更、撤销、冻结、恢复等操作，CRL 的签发与发布等，所有操作的通过或拒绝结果均应明确记录；

6）机房门禁控制等物理环境事件：包括业务人员、安全运维人员、外部人员等在不同安全区域的进出记录等。

（2）审计日志记录内容

每项审计日志至少应包含以下内容：事件发生时间、事件类型、事件内容或描述、操作人员身份、操作对象、操作结果或处理结果。对系统的关键操作应由操作人员进行电子签名。

5.4.2. 审计日志的保存期限

GDCA 妥善保存电子认证服务的审计日志，系统日志应至少保存至电子签名认证失效后五年，并实施严格的访问控制以防篡改和删除。

5.4.3. 日志审计内容及审计周期

GDCA 至少每季度对系统日志进行一次审计，审计、核实系统和操作人员的合规性，包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件，形成审计报告，并基于审计结果采取改进措施。

5.5. 记录归档

5.5.1. 归档记录的类型

GDCA 对以下几类事件进行归档记录，包括但不限于：

（1）证书申请材料和订户意愿；

（2）所有审计日志；

（3）密码设备全生存周期管理记录；

（4）密码设备的日常操作与使用记录；

（5）根证书或密钥生存周期管理相关的全部记录；

（6）证书认证系统运行日志；

（7）已识别的安全事件及处置记录；

（8）证书认证系统关键操作日志；

（9）电子认证服务过程中其他操作记录。

5.5.2. 归档记录的保存期限

订户相关档案、系统日志和审计记录至少保存至证书失效后 5 年。

5.5.3. 归档文件的保护

GDCA 采取必要的技术和管理措施保护归档记录，防止归档记录被未经授权访问、篡改、删除、损毁或泄露。

电子归档记录存储于安全的物理环境与数字环境中，并采取访问控制、身份鉴别、完整性校验、日志审计等保护措施。GDCA 建立归档数据备份机制，每周开展数据备份，确保归档记录在系统故障、设备损坏或灾害事件发生时能够有效恢复。

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。

GDCA 设立了专门的档案管理职能或指定专门管理部门，统一负责归档记录的收集、保存、调阅、备份和销毁等管理工作。GDCA 建立归档管理制度，明确了归档管理职责、操作流程、访问权限及安全要求。

5.6. 电子认证服务机构根证书密钥更替

GDCA 在以下情况下进行根密钥更替：

- 紧急更替：GDCA 发现密钥泄露或存在安全隐患，应立即启动密钥更替程序；
- 到期更替：在密钥到期前或前二年完成密钥更替。

GDCA 根证书密钥更替程序如下：

（1）密钥生成：在颁发或更换根证书时，遵循本 CP/CPS 第 6.2 节的规定，在安全可靠的环境中生成密钥对；

（2）根证书的发布：将新的 CA 公钥证书发布给证书订户和依赖方；

（3）旧密钥处理：在完成签名密钥更替后，按照 GB/T 25056-2018 第 8.2.4.3 条

规定的方式，销毁旧私钥及其备份，并保留相关操作记录。

5.7. 损害与灾难恢复

5.7.1. 业务连续性目标

为了及时响应和处理事故和损害发生的情况，GDCA 建立了一系列应急处理预案和事故处理方案，如 GDCA 系统故障处理规范、GDCA 重大事故应急预案、GDCA 系统备份与恢复方案等，承诺在业务系统因灾难或重大事故中断后，恢复时间目标（RTO）为 24 小时，恢复点时间目标（RPO）为 24 小时。

相关岗位的工作人员将按照业务连续性方案和相关制度的规定，积极实施抢修恢复计划和措施。

5.7.2. 事故和损害处理程序

（1）证书库的恢复过程

当证书库或相关系统受到损害时，GDCA 按照灾难恢复预案重建安全运行环境，并恢复证书库数据。恢复过程中，GDCA 将根据审计记录和备份数据识别受影响证书状态，必要时生成受影响证书或被撤销证书清单，并按照证书状态管理要求更新证书状态信息。对于涉及订户密钥管理的场景，GDCA 按照相关管理制度处理订户密钥及证书状态，并在必要时重新向订户签发和提供有效的证书。

（2）根密钥损害恢复

当根证书密钥材料发生损坏、不可用或其他影响正常使用的情况时，GDCA 启动根密钥恢复程序。恢复工作包括重建符合安全要求的运行环境、恢复根密钥材料或重新生成根密钥、建立新的信任链，并根据影响范围对受影响证书进行重新签发或替换。

在需要重新建立信任体系时，GDCA 将按照相关程序向订户及依赖方发布通知，并提供新的公钥证书及相关验证信息。

（3）其他关键资产恢复

GDCA 建立针对关键基础设施的恢复机制，包括但不限于：物理设施、计算资源、网络环境、业务系统及支撑软件、数据库及业务数据、密码设备及其他密钥材料。

GDCA 根据资产重要程度制定相应恢复方案，确保关键业务能够持续运行。

（4） 根私钥泄露应急处理

GDCA 建立了根私钥泄露应急处置机制，明确事件响应流程、响应时间要求、责任人员、处置步骤和上报机制。当发现根私钥发生泄露、丢失、被非法使用或其他影

响安全的情况时，GDCA 应立即启动应急响应程序，采取风险控制措施，开展事件调查，并按照法律法规及主管部门要求履行报告义务，安全事件报告及通报机制按照本 CP/CPS 第 5.9 节相关规定执行。

GDCA 每年至少组织一次根私钥泄露应急演练，并根据演练结果持续优化应急预案和处置流程。

（5）备份验证与灾难恢复演练

GDCA 定期验证备份设备、备份数据及恢复程序的有效性，包括备份恢复测试、数据完整性验证及功能验证等活动。GDCA 每年至少开展一次灾难恢复演练，验证灾难恢复预案、恢复流程及业务连续性目标的有效性，并根据演练结果及时完善相关管理制度和技术措施。

5.7.3. 灾难后的业务连续性能力

GDCA 定期验证备份的设备、数据可用性，包括备份恢复测试和功能验证，如定期从备份中随机抽取部分数据或系统配置文件进行恢复操作，每季度进行数据灾难恢复演练，每年进行一次灾难恢复演练和重大事故应急演练。

5.8. 电子认证服务机构终止

GDCA 因技术性原因或商业原因需要终止服务时，须：

（1）起草并发布 GDCA 终止声明，提前九十日通知证书订户、依赖方等相关实体，提前六十日向主管部门报告；

（2）与具有资质的电子认证服务业务承接单位签署承接协议，明确约定承接机构的工作范围与责任；

（3）向承接方移交密钥及相关关键数据，协调承接单位启动相关运营工作；

（4）停止证书状态服务并归档相关数据；

（5）停止其他电子认证相关服务并归档相关数据；

（6）停止密码设备并归档相关密钥数据；

（7）及时撤销或冻结业务管理员和业务操作员的操作权限；

（8）对所有存档文件记录进行整理和封存；

（9）对所有敏感文档和数据进行安全处理和封存；

（10）清除主机和密码硬件设备中的敏感数据；

（11）其他涉及 CA 运营的数据、密钥安全的操作；

（12）如果有与订户电子签名认证证书签发、管理相关的外部合作机构，应在 CP/CPS 中明确描述合作机构终止服务和通告相关的过程。

5.9. 重大事项报告

GDCA 建立了重大事项报告机制，对影响电子认证服务安全、连续运行、合规运营或订户合法权益的重大事项实施分级报告和管理。当发生或发现重大事项时，相关部门和人员应立即启动报告程序，按照内部管理制度及时向公司管理层报告，并根据法律法规、主管部门要求及事件影响情况，向上级机构和有关主管部门履行报告义务。重大事项包括但不限于：

（1）证书认证系统迁移或改造

包括系统软件、网络、部署的重大改变。符合以下任意之一：

- 机房迁移，或机房内服务区、管理区或核心区划设范围改变；
- 变更电子签名认证证书签发逻辑；
- 新增远程证书注册子系统；
- 新增、更改或者删除用于签发电子签名认证证书的证书链；
- 其他对电子认证服务安全、用户资料安全有影响的改变。

（2）重大安全事故

包括电子认证服务系统遭受黑客攻击、病毒入侵、数据泄露等，导致系统无法正常运行或数据安全性受到严重威胁的情形。符合以下任意之一：

- 证书签发及验证服务连续停机时间超 24h；
- 发生根证书密钥等关键数据泄露；
- 持续或较大范围未经授权的私钥访问记录或其他异常活动；
- 系统日志持续或较大范围显示异常操作(如非授权时间或网络地址访问敏感功能)。

（3）订户信息泄露事件

包括订户身份信息、证书申请资料等敏感数据被泄露等。符合以下任意之一：

- 个人信息泄露事件影响范围较广，造成一定的经济损失或客户投诉；
- 数据丢失导致无法恢复证书状态信息。

（4）合规性事件

包括不符合相关法律法规、标准或监管要求的情形。符合以下任意之一：

- 涉及电子认证服务的司法判定；

- 收到行政部门违规通知或处罚决定。

（5）人力资源类事件

包括一个月内核心管理层集体离职、大规模劳动纠纷、重大职场安全事件等。符合以下任意之一：

- 涉及 2 名及以上管理层人员或 10%以上可信人员的离职；
- 劳动纠纷参与人数超过员工总数 10%，且经法院或仲裁机构生效裁决确认由 CA 承担法律责任。

6. 认证系统技术安全控制

6.1. 技术安全管理制度要求

GDCA 已建立并实施覆盖电子认证服务全过程的技术安全管理制度，用于保障认证系统、密码系统、网络环境及密钥管理体系的安全、稳定与持续运行。技术安全管理制度覆盖但不限于以下方面：密钥生命周期安全管理、系统建设与开发安全管理、系统变更与发布管理、主机、数据库及应用安全管理、漏洞管理与安全加固、日志审计与安全监测、数据备份与恢复管理、业务连续性与灾难恢复管理。

GDCA 定期对技术安全管理制度的适用性、有效性及执行情况进行检查与完善，并提交安全策略委员会进行评审。安全策略委员会每年至少组织一次技术安全管理制度评审，根据法律法规、监管要求、技术发展及业务变化情况，对相关制度进行修订和优化。

6.2. 密钥对的生成与安装

6.2.1. 根证书密钥对的生成和安装

GDCA 根证书密钥对在物理隔离的安全环境中生成和安装。根密钥生成环境采用严格访问控制措施，与生产网络及互联网实施物理隔离，并采取视频监控、门禁控制、防拆封及安全审计等保护措施。

根证书密钥对采用经国家密码管理部门认可的硬件密码设备生成，密码设备满足国家有关密码安全管理及检测认证要求，能够提供密钥生成、存储、使用及访问控制等安全保护能力。

根证书密钥对的生成、备份、恢复及销毁操作实施 M 选 N 多人控制机制。其中：

- M 值不少于 5；
- N 值不少于 M 值的一半；

- 任一关键操作均须达到不少于 N 名授权人员共同参与方可完成。

参与操作的人员应经过授权和身份确认，职责相互分离，并按照最小权限原则实施管理。根证书密钥对相关操作须经安全策略委员会批准后方可实施。操作前应制定操作方案，明确参与人员、职责分工、操作步骤及安全控制要求。

根证书密钥对生成、备份、恢复、销毁及安装全过程应通过录音录像方式进行完整记录，并同步保留操作日志、审批记录、见证记录及相关审计材料。

根证书密钥对生成完成后，应按照安全操作规程完成根证书安装，并对安装结果进行验证，确保根证书及相关密码参数正确部署。

上述录音录像资料及相关操作记录的保存期限不少于操作完成后十年。

6.2.2. 订户密钥对生成和交付

GDCA 根据不同业务场景，采用符合国家有关密码管理及电子认证管理要求的方式实现订户签名密钥对的生成、交付及控制，并确保订户对签名私钥具有合法、有效且独占的控制权。GDCA 目前支持以下订户签名密钥对生成及控制方式：

（1）订户本地生成和存储

在订户本地生成模式下，订户签名密钥对由订户持有的符合国家安全标准要求的密码模块生成和存储，私钥不可导出。CA 不获取、不保存订户签名私钥。

用于生成和存储订户签名私钥的密码设备应符合国家有关密码安全管理要求，并具备访问控制、防篡改及密钥保护能力。

对于由订户本地密码模块生成和控制的签名私钥，GDCA 不获取、不保存订户签名私钥，也不记录订户本地签名操作过程。

（2）GDCA 生成及托管

在 GDCA 生成及托管模式下，订户签名密钥对由 GDCA 在符合相关安全标准的安全环境中生成，并采用密码技术、安全认证机制及访问控制措施保障订户对签名私钥的独占控制权。GDCA 通过身份认证、动态授权、多因素认证、或其他安全控制机制，确保任何组织或个人无法在未经订户授权的情况下独立使用订户签名私钥完成电子签名操作。

该模式下，GDCA 完整记录与订户签名私钥管理及使用相关的操作日志，包括但不限于：密钥生成、使用、更新、恢复、销毁、签名授权操作。

日志记录内容包括操作时间、操作方式、操作主体、操作结果及相关审计信息。相关日志采取防篡改保护措施，并自对应证书失效之日起至少保存五年。

（3）其他创新性保护方案

对于经主管部门认可的其他创新性保护方案，GDCA 可根据业务发展及监管要求，在履行相应管理程序后实施，并确保订户签名私钥的安全性、完整性及订户独占控制权符合国家有关规定。CA 在采用相关创新性保护方案前，将依据主管部门要求开展安全评估、合规论证及风险控制，并在相关业务规则、技术规范及操作流程中明确具体控制措施。

此外，对于仅用于加密用途的证书，证书订户的加密密钥对由 GDCA 代订户申请生成，并由 GDCA 进行管理。当证书订户需要恢复加密密钥时，按照 GDCA 流程，接受订户的申请为订户恢复相应的加密密钥。

6.3. 私钥保护和密码模块工程控制

6.3.1. CA 私钥保护和密码模块工程控制

GDCA 根证书私钥采用通过国家密码主管部门认可的密码产品进行保护，相关密码模块符合国家有关密码安全管理要求，并满足 GB/T 37092-2018 第 5 章关于密码模块安全的相关要求。根证书私钥在符合安全控制要求的密码设备中生成、存储和使用，私钥以受保护形式存在，不以明文形式导出或保存。

GDCA 对根证书私钥实施严格的分割保护机制，采用多人分管、分权控制及密钥分片等安全措施，确保任何单一人员无法获取或控制完整根证书私钥。

根证书私钥备份按照安全管理要求实施分割保存，由经授权的密钥管理员分别保存在具备防盗及访问控制措施的独立安全场所中。

根证书私钥及其备份的访问、使用、恢复及销毁等操作均应经过授权审批，并记录完整审计日志。相关操作应符合职责分离、最小权限及多人控制原则。GDCA 定期对密码模块、根证书私钥保护状态及备份保管情况进行安全检查和审计，确保根证书私钥持续处于安全受控状态。

6.3.2. 订户私钥保护和密码模块工程控制

GDCA 根据不同业务场景，采用符合国家有关密码管理及电子认证管理要求的措施，对订户签名私钥进行安全保护，并确保订户对签名私钥具有合法、有效且独占的控制权。

（1）订户持有模式

对于由订户持有的签名私钥，订户签名私钥应由订户持有的符合国家安全标准要求的密码模块生成、存储和使用，私钥不可导出。GDCA 通过订户协议或其他方式，要求

订户采取必要的安全保护措施，防止订户签名私钥及其激活数据发生丢失、泄露、更改或未经授权的使用。

（2）GDCA 受托保管模式

在订户授权的情况下，GDCA 可采用符合国家有关要求的电子签名模式，为订户提供签名私钥托管服务。GDCA 采用的电子签名模式包括云签名或其他符合监管要求的安全电子签名模式。

GDCA 采用密码技术、身份认证、访问控制、多因素认证及安全审计等控制措施，对订户签名私钥进行保护，并定期开展安全评估，确保相关技术和管理措施持续有效。

每次调用订户签名私钥进行电子签名操作前，均须获得订户明确授权。GDCA 完整记录订户授权过程及签名操作相关记录，并采取防篡改措施进行保护。

GDCA 向订户提供关于签名私钥、激活数据及电子签名安全使用的指导与建议，提示订户妥善保管身份认证信息及激活数据。

GDCA 采用的电子签名模式及相关安全控制措施符合国家有关标准要求，或采用经主管部门认可的其他方式实施。

（3）其他经认可的方式

对于经主管部门认可的其他订户私钥保护方式，GDCA 将在履行相应安全评估、风险控制及管理程序后实施，并在本 CP/CPS 中明确具体控制措施。

6.4. 密钥对管理的其他方面

6.4.1. 公钥归档

GDCA 对已签发的公钥证书及相关证书状态信息进行定期归档保存，公钥证书归档内容包括但不限于：已签发证书、吊销证书、证书状态信息等。

GDCA 按照规定周期对公钥证书信息进行归档，归档操作的最大间隔不超过六个月。归档数据采取访问控制、防篡改及备份保护措施。

6.4.2. 证书操作期和密钥对使用期限

无论是 CA 证书还是订户证书，在证书有效期届满后，其对应签名私钥均不得继续用于电子签名操作。GDCA 通过系统控制、证书状态管理及密钥生命周期管理措施，防止过期签名私钥被继续使用。

根证书密钥对、CA 证书密钥对、订户证书密钥对及其他用于电子认证服务的密钥均应设置明确的有效期限，并根据业务类型、风险等级及国家有关要求进行管理。

各类密钥最长有效期如下：

密钥类型	最长有效期
根证书密钥对	30 年
中级 CA 证书密钥对	13 年
订户证书密钥对	5 年
时间戳签名密钥对	5 年
OCSP 签名密钥对	5 年

6.5. 激活数据

6.5.1. 激活数据的产生和安装

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

CA 私钥的激活数据，必须按照有关密钥激活数据分割和密钥管理办法的要求，严格进行生成、分发和使用。订户私钥的激活数据，包括用于下载证书的口令、USB Key、IC 卡的登陆口令等，都必须在安全可靠的环境下随机产生。

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

所有的保护口令都应该是不容易被猜到的，应该遵循以下几个原则：

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

6.5.2. 激活数据的保护

对于 CA 私钥的激活数据，必须将激活数据按照可靠的方式分割后由不同的可信人员掌管，而且掌管人员必须符合职责分割的要求。

订户的激活数据必须在安全可靠的环境下产生，必须进行妥善保管，或者记住以后

进行销毁，不可被他人所获悉。如果证书订户使用口令或 PIN 码保护私钥匙，订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书订户使用生物特征保护私钥，订户也应注意防止其生物特征被人非法窃取。同时为了配合业务系统的安全需要，应该经常对激活数据进行修改。

在 CA 托管订户签名私钥的业务场景下，订户签名私钥调用所需激活数据应与签名授权过程绑定，并具备动态验证、时效控制或一次性使用等安全特性。每次调用订户签名私钥进行电子签名操作前，均须获得订户明确授权。

6.5.3. 激活数据的其他方面

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

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

考虑到安全因素，对于申请证书的订户激活数据的生命周期，规定如下：

1. 订户用于申请证书的口令，申请成功后失效。

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

6.6. 计算机安全控制

6.6.1. 特别的计算机安全技术要求

GDCA 建立并实施符合 GB/T 25056-2018 第 8.2 条要求的计算机安全控制体系，对电子认证服务相关的信息系统、服务器、操作终端及网络环境实施安全管理和技术控制，降低恶意代码、系统漏洞及未经授权访问等安全风险。具体包括但不限于以下方面：

- GDCA 建立补丁和漏洞管理机制，定期对系统补丁、漏洞修复情况及安全配置进行检查。系统升级补丁至少每半年检查一次，并记录系统升级、补丁安装、审批及实施过程。
- 对于已停止官方补丁支持或存在较高安全风险的系统，GDCA 采取网络隔离、访问控制、功能限制、最小化服务、加强监测等安全防护措施，并制定系统更替或升级计划。
- GDCA 在电子认证服务相关服务器、操作终端及其他重要信息处理设备中部署

防病毒或恶意代码防护软件，并保持防护机制持续有效。

- 病毒库定期进行更新，病毒库更新时间间隔最长不超过 7 天；在出现重大安全风险、重大病毒事件或高危漏洞时，及时进行更新。
- GDCA 定期对服务器、操作终端及相关信息系统进行病毒扫描和恶意代码检测，病毒扫描时间间隔最长不超过 7 天；对于重要系统或高风险区域，可根据安全需要提高扫描频率。
- GDCA 对恶意代码检测、补丁升级、安全防护及相关安全事件处理过程保留审计记录。

6.6.2. 计算机安全评估

GDCA 的认证系统，通过了国家密码管理局的安全性审查。

GDCA 定期对电子认证服务相关信息系统开展计算机安全检查和安全评估，评估内容包括系统安全配置、漏洞管理、恶意代码防护、访问控制、安全审计及安全策略执行情况等。GDCA 根据安全评估结果，及时采取漏洞修复、安全加固、补丁升级、风险整改及其他必要安全措施，确保系统持续安全运行。

对于发现的重大安全隐患或高风险问题，GDCA 应及时进行风险分析、整改和跟踪验证，并根据需要采取加强监测、限制访问、隔离运行或系统替换等控制措施。

6.7. 生存周期技术控制

GDCA 建立并实施符合 GB/T 25056-2018 第 10 章、第 11 章及第 12 章要求的系统开发控制体系，对电子认证服务相关系统的需求分析、设计、开发、测试、部署、运行及维护等过程实施安全管理和技术控制。

6.7.1. 系统开发控制

GDCA 的软件设计和开发过程遵循以下原则：

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

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

发控制。

6.7.2. 安全管理控制

GDCA 认证系统的信息安全管理，严格遵循国家密码管理局的有关运行管理规范进行操作。GDCA 认证系统的使用具有严格的控制措施，所有的系统都经过严格的测试验证后才进行安全和使用，任何修改和升级会记录在案并进行版本控制、功能测试和记录。GDCA 还对认证系统进行定期和不定期的检查和测试。

GDCA 采用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具备在更加严格的安全控制机制下，进行设备的检验、安装和验收。

GDCA 认证系统所有的软硬件设备升级以后，废旧设备在进行处理时，首先必须确认其是否有影响安全的信息存在。

6.7.3. 生存周期的安全控制

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。

6.8. 网络安全控制

GDCA 建立并实施了符合 GB/T 25056-2018 第 5.3.8 条要求的网络安全控制体系，对电子认证服务相关网络环境实施安全管理和技术控制。

6.8.1. 网络结构与边界安全控制

GDCA 网络结构根据 GB/T 25056-2018 附录 A 中“图 A.2 RA 采用 B/S 模式时 CA 的网络结构示意图”进行设计和部署，并结合电子认证服务实际业务场景，对不同网络区域实施边界隔离、访问控制及安全防护措施。

GDCA 在电子认证服务相关 Web 服务及重要网络边界部署防火墙、Web 应用防火墙（WAF）、入侵检测或入侵防御系统（IDS/IPS）、内容过滤及其他必要的网络安全防护措施，防止未经授权访问、网络攻击、恶意代码传播及其他安全风险。

GDCA 建立并维护了网络拓扑图，网络拓扑图应包括网络设备、连接关系、安全区域划分及安全边界等信息，并根据网络变更情况及时更新，确保与机房实际网络环境保持一致。

6.8.2. 网络访问控制

GDCA 建立了网络访问控制机制，对电子认证服务相关信息系统、网络设备及数据库实施访问控制和权限管理。建立了针对证书签发子系统及数据库的访问白名单机制，仅允许经授权的证书注册子系统必要功能模块及必要管理设备进行访问。

GDCA 建立了针对证书注册子系统及数据库的访问白名单机制，限制未经授权的网络访问和系统连接。

根据业务安全需求，GDCA 对不同网络区域、业务系统及管理终端实施访问控制、安全隔离及最小权限管理。

6.8.3. 网络监控与安全审计

GDCA 建立网络安全监控和日志分析机制，对电子认证服务相关系统、网络设备及安全设备运行状态进行持续监测。GDCA 定期对系统日志、安全日志及网络设备日志进行分析，分析内容包括但不限于系统异常、未授权访问尝试、资源使用异常、配置变更及其他安全事件。

对于发现的异常行为、安全风险或攻击事件，GDCA 应及时进行分析、处置和跟踪，并根据需要采取访问限制、阻断、隔离、加固或其他安全控制措施。

6.9. 时间戳

GDCA 提供符合 RFC 3161、RFC 5816 规范的时间戳服务，用于为电子签名及相关业务提供可信时间证明。时间戳服务通过时间戳服务器（TSA）向申请者签发时间戳标记。

GDCA 采用安全可靠的时间源，并通过访问控制、安全审计及系统安全防护等措施保障时间戳服务安全稳定运行。GDCA 业务系统的系统时间通过 NTP 协议与时间戳服务进行同步，以保证系统时间的一致性和准确性。

7. 证书、证书撤销列表和在线证书状态协议

7.1. 证书

GDCA 签发的电子签名认证证书采用符合 GB/T 20518 及 ITU-T X.509v3 标准的数字证书格式。证书包含证书版本号、证书序列号、签名算法标识、颁发者名称、订户名称、证书有效期、订户电子签名验证数据、证书扩展项以及 CA 电子签名等内容。

GDCA 所签发证书结构基本域如下：

域	值或值的限制
版本	指明 X.509 证书的格式版本，值为 V3
序列号	证书的唯一标识符
签名算法	签发证书时所使用的签名算法（见 CP/CPS 第 7.1.3 节）
签发者	签发者的甄别名
有效起始日期	基于国际通用时间(UTC)，和北京时间同步，按 RFC 5280 要求编码
有效终止日期	基于国际通用时间(UTC)，和北京时间同步，按 RFC 5280 要求编码。有效期限的设置符合本 CP/CPS 规定的限制。
主题 DN	证书持有者或实体的甄别名如下： CA 根证书 DN：CN、O、C。 中级 CA 证书 DN：CN、O、C。 订户机构证书 DN：CN、O、OU（可选）、L（可选）、S（可选）、C。 订户机构个人证书 DN：CN、O、OU（可选）、L（可选）、S（可选）、C。 订户设备证书 DN：CN、O（可选）、C。 订户个人证书 DN：CN、L（可选）、S（可选）、C。
公钥	根据 RFC 5280 编码，使用 CP/CPS 7.1.3 中指定的算法，密钥长度满足 CP/CPS 指定的要求。

7.1.1. 版本号

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

7.1.2. 证书扩展项

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

7.1.2.1. 根证书

1. 基本约束

根证书须设置该扩展项，且该扩展项为关键扩展项，主体类型被设为 CA，“pathLenConstraint”字段未设置。

2. 密钥用法

根证书须设置该扩展项,且该扩展项关键扩展项,用法设置为 KeyCertSign,CRLSign。根证书对应的私钥不用于签署 OCSP 响应。

3. 证书策略

该扩展项未设置。

4. 增强型密钥用法

该扩展项未设置。

5. 主题密钥标识符

根证书须设置该扩展项,且该扩展项不应标记为关键扩展项,它的值应该包含在根证书签发的证书中的 authorityKeyIdentifier 扩展的 keyIdentifier 字段中。

7.1.2.2. 中级 CA 证书

1. 证书策略

中级 CA 证书中须设置该扩展项,且不得为关键扩展项,有关具体的策略标识符的信息请见本 CP/CPS 的第 1.5.1.2 节。

2. CRL 分发点

中级 CA 证书中须设置该扩展项,且不得为关键扩展项,该扩展项须包含 CA CRL 服务的 HTTP 地址。

3. 颁发机构信息访问

中级 CA 证书可设有颁发机构信息访问扩展项,若设置,则不得为关键扩展项,此扩展中会包含指向此 CA 证书签发者证书的 HTTP 地址(AccessMethod=1.3.6.1.5.5.7.48.2)和指向 CA OCSP 服务的 HTTP 地址(AccessMethod=1.3.6.1.5.5.7.48.1)。

4. 基本约束

中级 CA 证书须设置该扩展项,且该扩展项为关键扩展项,主体类型被设为 CA,"pathLenConstraint"字段可设置。

5. 密钥用法

中级 CA 证书中须设置该扩展项,且为关键扩展项,且必须设置 KeyCertSign,CRLSign 用法。中级 CA 证书对应的私钥不用于签署 OCSP 响应。

6. 颁发机构密钥标识符

中级 CA 证书须设置该扩展项,且不得为关键扩展项。该扩展项仅包含 KeyIdentifier

字段。

7. 主题密钥标识符

中级 CA 证书须设置该扩展项，且该扩展项不应标记为关键扩展项，它的值应该包含在中级 CA 签发的证书中的 authorityKeyIdentifier 扩展的 keyIdentifier 字段中。

7.1.2.3. 订户证书

1. 证书策略

订户证书中须设置该扩展项，且不得为关键扩展项，包含主管部门制定的相应等级证书策略 OID，并可包含 GDCA 制定或遵循的其他证书策略 OID。有关具体的策略标识符的信息请见本 CP/CPS 的第 1.5.1.2 节。

2. CRL 分发点

可设置该扩展项，若设置，则该扩展项为非关键扩展。此扩展项中会包含指向 CA CRL 服务的 HTTP URL 地址。

3. 颁发机构信息访问

可设有颁发机构信息访问扩展项，若设置，则不得为关键扩展项，此扩展中会包含指向此 CA 证书签发者证书的 HTTP 地址（AccessMethod=1.3.6.1.5.5.7.48.2）和指向 CA OCSP 服务的 HTTP 地址（AccessMethod=1.3.6.1.5.5.7.48.1）。

4. 基本约束

可设置该扩展项，若设置，则此扩展中“cA”字段须设置为“False”。

5. 密钥用法

订户证书可设置该扩展项，若设置，则密钥用法不得设置为 keyCertSign 及 cRLSign。

6. 颁发机构密钥标识符

订户证书须设置该扩展项，且不得为关键扩展项。该扩展项仅包含 KeyIdentifier 字段。

7. 主题密钥标识符

订户证书须设置该扩展项，且该扩展项不应标记为关键扩展项，它应该包含一个从订户证书中的公钥派生出来的值。

7.1.2.4. 所有证书

GDCA 除了使用 RFC5280 定义的标准项和标准扩展项以外，还可使用自定义扩展项，例如，针对不同的证书应用服务需求，GDCA 可灵活定义一些扩展项，包括但不限于如下扩展项：

1. 统一社会信用代码号：用于表示企业的统一社会信用代码。
2. 信任服务号：证书颁发机构产生用于标识订户的唯一编号。
3. 个人身份证号码：用于表示居民身份证的唯一编号。

7.1.3. 算法对象标识符

GDCA 签发的数字证书使用以下相关算法之一：

sha256RSA withRSAEncryption	1.2.840.113549.1.1.11
SM3withSM2Encryption	1.2.156.10197.1.501

7.1.4. 名称形式

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。

7.1.5. 名称限制

GDCA 可根据 RFC5280 来使用名称限制扩展项，以限制中级 CA 证书的业务应用范围。

7.1.6. 证书策略对象标识符

证书策略对象标识符同本 CP/CPS 第 1.5.1.2 节。

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规则

不适用。

7.2. 证书撤销列表

GDCA 发布的证书撤销列表（CRL）采用符合 GB/T 20518-2018 第 5.3 章要求的格式。CRL 中包括 CRL 版本号、签发者名称、更新时间、下次更新时间、被撤销证书序列号、撤销时间及 CA 电子签名等内容。GDCA 按照本 CP/CPS 第 4.9.7 节的规则及时发

布和更新 CRL，并提供证书状态查询服务。

7.2.1. 版本

GDCA 的证书撤销列表采用 X.509 v2 格式。

7.2.2. CRL 和 CRL 条目扩展项

GDCA 的证书撤销列表（CRL）是一个带有时间戳并且经过数字签名的已撤销证书的列表。CRL 的签发者是 CA，GDCA 通过发布 CRL 提供它所签发的数字证书的状态信息。

（1）CRL 的版本号：用来指定 CRL 的版本信息，GDCA 采用的是同 X.509 V3 证书对应的 CRL V2 版本。

（2）签名算法：GDCA 采用 sha1 RSA、sha256RSA、sha256ECDSA 及 SM2 签名算法。

（3）颁发者：指定签发机构的 DN 名，由国家、省、市、机构、单位部门和通用名等组成。

（4）生效时间：指定一个日期/时间值，用以表明本 CRL 发布的时间。

（5）更新时间：指定一个日期/时间值，用以表明下一次 CRL 将要发布的时间（本标准强制使用该域）。

（6）撤销证书列表：指定已经撤销的证书列表。本列表中含有证书的序列号和证书被撤销的日期和时间。

（7）颁发机构密钥标识符（Issuer Unique Identifier）：本项标识用来验证在 CRL 上签名的公开密钥。它能辨别同一 CA 使用的不同密钥。

7.3. 在线证书状态协议

GDCA 提供在线证书状态服务（OCSP），用于向订户和依赖方提供数字证书状态查询服务。在线证书状态服务符合 GB/T 19713-2025 第 7 章的相关要求，能够对证书的有效、吊销、未知等状态进行查询和响应。同时也符合 IETF PKIX 工作组开发的在线证书状态协议 (Online Certificate Status Protocol，OCSP，RFC6960)。在 GDCA 官方网站下载 OCSP 查询客户端并按照 GDCA 官方网站发布的 OCSP 操作说明进行配置，即可使用 GDCA 的在线证书状态查询服务。GDCA 签发的 OCSP 响应至少包含以下所述的 OCSP 机构基本域和内容：

（1）Version：客户端使用的 OCSP 协议的版本号；GDCA 的在线证书状态协议为

v1 版。

（2）signatureAlgorithm：签发 OCSP 的算法。

（3）responderID：签发 OCSP 的实体。签发者公钥的 SHA1 数据摘要值和证书甄别名。

（4）producedAt：OCSP 响应生成的日期和时间。

（5）Signature：OCSP 响应消息的数字签名。

（6）Nonce(一次性随机数)：在状态请求消息中的每一个 requestExtensions 变量和响应消息中的 responseExtension 变量中包含一次性随机数，防止重放攻击。

（7）证书状态：证书的最新状态，包括有效、撤销和未知。

7.3.1. 版本号

RFC6960 定义的 OCSP 版本。

7.3.2. OCSP 请求和响应处理

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

- 信息正确格式化
- 响应服务器被配置提供请求服务
- 请求包含了响应服务器需要的信息，如果任何一个先决条件没有满足，那么 OCSP 服务端将产生一个错误信息；否则的话，返回一个确定的回复

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

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

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

- 未正确格式化的请求（malformedRequest）
- 内部错误（internalError）

- 请稍后再试（trylater）
- 需要签名（sigRequired）
- 未授权（unauthorized)

7.3.3. OCSP 扩展项

不适用。

8. 认证机构审计及相关评估

8.1. 审计评估制度

GDCA 建立并实施了审计评估制度，对电子认证服务相关业务活动、系统运行情况及管理体系的合规性进行监督与检查，以确保持续符合国家相关法律法规、标准规范及主管部门要求。审计评估类型至少包括认证业务审计和全面符合性评估。认证业务审计用于对日常电子认证业务执行过程的合规性进行检查，全面符合性评估用于对电子认证服务体系整体运行及制度执行情况进行系统性评估。

审计评估原则上定期开展，全面符合性评估每年至少开展一次，并可在发生重大系统变更、安全事件、监管要求或内部控制需要时启动专项审计评估。

参与审计评估的人员应具备信息安全、电子认证或相关专业背景，且具备相应的审计或评估能力。如由外部机构实施审计评估，应选择具备相应资质、独立性和专业能力、熟悉电子认证相关标准与规范的第三方机构。

审计评估范围涵盖电子认证业务流程、人员管理、系统与网络安全、密码管理及相关管理制度执行情况，审计评估方法包括文档审查、系统检查、日志分析、抽样检查及必要的现场核查等。

8.2. 认证业务审计

GDCA 对电子认证业务开展认证业务审计，以验证业务流程及操作执行的合规性和一致性。认证业务审计每季度实施一次，审计周期可根据业务风险情况进行调整。审计内容包括但不限于证书申请、证书续期、密钥更新、证书更新、证书撤销及证书冻结等业务流程中订户告知、身份查验、意愿确认、协议签署及相关资料保存的合规性。

认证业务审计采用抽样审计方式实施，抽样比例不低于已签发证书的 1‰。

对于审计发现的问题，GDCA 应及时通知相关部门和人员进行整改，并对整改过程及结果进行跟踪验证，确保整改措施有效落实。

8.3. 全面符合性评估

GDCA 建立并实施了全面符合性评估机制，对电子认证服务体系整体运行情况进行系统性检查与评估。全面符合性评估每年至少开展一次，并可根据监管要求、重大变更或风险事件适当增加评估频率。

评估内容包括但不限于年度电子认证服务开展情况、电子认证服务许可条件符合性情况以及认证规则和证书策略符合性情况等。

全面符合性评估可采用抽样方式实施，抽样比例应不低于认证业务审计抽样要求。

对于评估发现的问题，应及时通知相关责任部门进行整改，并对整改情况进行跟踪验证，确保整改措施落实到位。

GDCA 应于每年 1 月底前将上一年度全面符合性评估报告报送主管部门。

9. 法律责任和其他业务条款

9.1. 费用

GDCA 可根据提供的电子认证相关服务向本机构的证书订户收取费用，具体费用将取决于市场规则和相关管理部门的规定。GDCA 根据市场状况，结合电子认证服务运营成本、系统建设及维护投入、服务对象、服务内容等因素，开展服务成本的核算，根据核算结果制定各项服务收费标准，针对不同订户群体推出不同的收费策略或优惠措施。

9.1.1. 证书颁发和更新费用

GDCA 根据制定的价格策略确定证书颁发和更新服务收费标准，并通过官方网站或其他适当方式向订户公布。GDCA 可根据不同类型订户、证书类型、服务期限及业务场景等因素制定差异化收费标准或优惠措施。

如 GDCA 与订户签署的服务协议中约定的证书颁发或更新费用与 GDCA 公布的收费标准不一致，以双方协议约定的费用为准。

9.1.2. 证书访问及查询费用

在证书有效期内，对该证书信息进行访问及查询，目前 GDCA 不收取费用。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。

如果证书访问及查询的收费政策有任何变化，GDCA 将会及时在网站

https://www.gdca.com.cn 上予以公布。

9.1.3. 证书撤销或状态信息的查询费用

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

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

9.1.4. 电子签名相关费用

GDCA 根据电子签名服务运营、安全管理及服务保障需要，制定电子签名相关服务收费标准。电子签名相关费用可包括电子签名服务费用、签名验证服务费用以及签名验证报告服务费用等。

9.1.5. 其他服务费用

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

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。

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。

9.1.6. 退款策略

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/CPS 所规定的责任或其它重大义务，订户可以要求 GDCA 撤销证书并退款。在 GDCA 撤销了订户的证书后，GDCA 将立即把订户为申请该证书所支付的费用全额退还给订户。

此退款策略不限制订户得到其它的赔偿。

相关收费标准、服务说明及退款规则等信息，可通过 GDCA 官方网站、业务受理渠道、服务协议或其他适当方式向社会公布。

9.2. 财务责任

9.2.1. 保险范围

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

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

对于特定应用场景下的证书业务，GDCA 也可以根据具体情况另行约定证书赔偿金额上限。

GDCA 建立了电子认证服务赔付保障机制，设立了赔付专项备用资金，用于保障电子认证服务相关赔付责任的履行。GDCA 赔付专项备用资金来源于公司自有资金，额度不低于上一年度营业收入的 1.5%，资金实行专账核算管理。

9.2.2. 其他资产

不适用。

9.2.3. 对最终实体的保险或担保

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

（1）GDCA 所有的赔偿义务不得超出本节 9.2.1 中规定的保险范围，赔偿金额不得高于赔偿金额上限，赔偿金额上限可以由 GDCA 根据情况重新制定，GDCA 会将重新制定后的情况立刻通知相关当事人。

（2）GDCA 只有在证书有效期限内承担损失赔偿责任。

9.2.4. 责任免除

有下列情形之一的，应当免除 GDCA 之责任：

（1）订户在申请和使用 GDCA 数字证书时，有违反如下义务之一的：

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

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

- 自然现象或者自然灾害，包括地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；
- 社会现象、社会异常事件或者政府行为，包括政府颁发新的政策、法律和行政法规，或战争、罢工、骚乱等社会异常事件。

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

- 不可抗力；
- 关联单位如电力、电信、通讯部门而致；
- 黑客攻击；
- GDCA 无法预见的突发设备或网络故障。

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

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

9.3. 业务信息保密

9.3.1. 保密信息范围

在 GDCA 提供的电子认证服务中，以下信息视为保密信息：

1）订户的签名私钥、解密私钥、激活数据及相关密钥材料；

2）证书申请资料、身份验证资料、协议资料及业务办理过程中形成的相关信息；

3）审计记录，包括本地日志、服务器日志、归档日志及其他安全审计信息；

4）GDCA 及注册机构（RA）保存的个人、机构及业务相关信息；

5）其他依法、依约或 GDCA 认为需要保密的信息。

9.3.2. 不属于保密的信息

GDCA 将以下信息视为不保密信息：

- 由 GDCA 签发的证书和 CRL 中的信息。
- 已公开发布的 CP/CPS 及相关公开信息。
- GDCA 许可，只有 GDCA 订户方使用，在 GDCA 网站公开发布的信息。
- 其他：依法应公开的信息。

9.3.3. 保护保密信息的责任

GDCA 有妥善保管与保护本节 9.3.1 中规定的保密信息的责任与义务。GDCA 采取访问控制、权限管理、安全审计及其他必要安全措施，对业务信息进行保护。

9.4. 个人隐私保护

9.4.1. 隐私保密方案

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

进行查询。

GDCA 按照国家有关法律法规及 GB/T 35273 等相关标准要求，对电子认证服务过程中涉及的个人隐私信息进行保护，并采取必要的管理和技术措施防止个人信息被未经授权访问、泄露、篡改或毁损。GDCA 在开展电子认证服务过程中，按照合法、正当、必要原则收集、使用、保存和处理个人信息，并仅在实现电子认证服务目的所必需的范围内处理相关信息。

GDCA 通过访问控制、权限管理、安全审计、加密保护及安全传输等措施，加强对个人隐私信息的安全保护，并对相关信息实行分类管理。除法律法规要求、监管要求、司法机关要求或经个人信息主体授权外，GDCA 不向任何第三方披露个人隐私信息。

9.4.2. 作为隐私处理的信息

除证书中已经公开的信息、证书状态信息以及依法应公开的信息外，订户提供的其他基本信息将被视为隐私信息进行保护。GDCA 定义以下信息属于订户的隐私信息：

- 订户的有效证件号码如身份证号码、统一社会信用代码等身份识别信息。
- 订户的联系电话。
- 订户的通信地址和住址。
- 订户的银行帐号。
- 订户提交的身份证明文件、影像资料、生物识别信息及身份核验信息。
- 订户在证书申请、使用及管理过程中形成的业务记录及相关信息。
- 法律法规规定或 GDCA 认为需要保护的其他个人隐私信息。

9.4.3. 不被视为隐私的信息

GDCA 定义包括但不限于以下信息，在符合证书应用要求、订户授权或法律法规规定的情况下，可作为公开信息进行披露：

- 订户姓名、机构名称等证书主体信息。
- 证书序列号、证书有效期、证书用途等证书公开信息。
- 证书状态信息，包括 CRL 及 OCSP 状态信息。
- 已公开发布的 CP/CPS 及相关公开信息。
- 法律法规规定应公开的信息。

9.4.4. 保护隐私的责任

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

9.4.5. 使用隐私信息的告知与同意

GDCA 在开展电子认证服务过程中，将按照合法、正当、必要原则收集、使用和处理订户个人信息，并采取必要的管理和技术措施保护已存储的个人隐私信息安全。

GDCA 将在证书申请、业务办理或相关服务过程中，采用协议、业务规则、服务页面或其他适当方式向订户告知个人信息的收集、使用及保护规则，并根据法律法规要求取得订户同意或授权。除法律法规规定、监管要求、司法机关要求或经订户授权外，GDCA 不会向未经授权的第三方提供除证书公开信息外的订户个人信息。

9.4.6. 依法律或行政程序的信息披露

在符合法律法规要求、监管要求、司法机关或其他有权机关依法提出要求的情况下，GDCA 可按照法定程序披露与电子认证服务相关的信息。可披露的信息包括但不限于：

- 订户身份信息及证书申请资料。
- 证书签发、使用、更新、撤销等业务记录。
- 相关系统日志、审计记录及业务操作记录。
- 法律法规要求提供的其他信息。

GDCA 在进行信息披露时，将按照法律法规及内部管理要求，对披露范围、用途和流程进行控制，并采取必要措施保护相关信息安全。

9.4.7. 其他信息披露情形

在电子认证服务过程中，如因业务办理、客户服务、证书交付、技术支持或其他服务需要，GDCA 可在实现相关服务目的所必需的范围内，将订户相关信息提供给合作服务方。

9.5. 知识产权

GDCA 依法享有其电子认证服务过程中形成或使用的 CP/CPS、技术文档、软件系统、服务平台、商标标识、服务名称及相关资料的著作权、商标权、专利权及其他知识产权。

- GDCA 享有并保留对证书以及 GDCA 提供的所有软件的全部知识产权。

- GDCA 对数字证书系统软件具有所有权、名称权、利益分享权。
- GDCA 网站上公布的一切信息均为 GDCA 财产，未经 GDCA 书面允许，他人不能转载用于商业行为。
- GDCA 发行的证书和 CRL 均为受 GDCA 支配的财产。
- 对外运营管理策略和规范为 GDCA 财产。
- 用来表示目录中 GDCA 域中的实体的甄别名（以下简称 DN）以及该域中颁发给终端实体的证书，均为 GDCA 的财产。

9.6. 陈述与担保

9.6.1. 电子认证服务机构的陈述与担保

GDCA 在提供电子认证服务活动过程中的承诺如下：

- 按照国家有关法律法规、主管部门要求、CP/CPS 开展电子认证服务活动。
- 签发的数字证书符合本 CP/CPS 的要求。
- 按照本 CP/CPS 规定对证书申请人的身份、申请资料及相关信息进行审核和验证。
- 验证证书申请行为已经获得申请人或相关授权主体的合法授权。
- 确保证书中所包含信息在证书签发时经过审核验证，并在已验证范围内保持准确性。
- 按照本 CP/CPS 要求及时签发、更新、撤销或管理数字证书。
- 在发现影响证书可信性、有效性或安全性的情况时，及时采取相应处理措施，并在必要时通知订户。
- 建立并维护证书状态服务系统，向依赖方提供证书状态查询服务。
- 建立并维护证书撤销列表（CRL）及在线证书状态服务（OCSP）。
- 对已经签发且未过期证书的状态信息提供持续公开查询服务。
- 按照法律法规及相关规定妥善保存电子认证服务相关资料和记录。
- 依法保护订户信息及个人隐私信息安全。

9.6.2. 注册机构的陈述与担保

GDCA 的注册机构在参与电子认证服务过程中的承诺如下：

- 按照国家有关法律法规、GDCA CP/CPS 要求开展注册审核及相关业务。

- 按照 GDCA 规定对证书申请资料、申请人身份及相关信息进行审核。
- 按照业务流程要求，及时向 GDCA 提交证书申请、更新、撤销等业务请求。
- 妥善保存业务办理过程中形成的相关资料和记录，并配合 GDCA 开展审计、检查及合规管理工作。
- 采取必要的安全管理措施，保护业务系统、申请资料及订户信息安全。

9.6.3. 订户的陈述与担保

订户一旦接受 GDCA 签发的证书，即视为其已阅读、理解并同意遵守本 CP/CPS 及订户协议，并作出以下承诺：

- 证书申请、使用及管理过程中提供真实、准确、完整的信息，并及时更新相关信息。
- 合法使用数字证书及相关服务，不将证书用于法律法规禁止或未经授权的用途。
- 妥善保管证书私钥、激活数据及相关安全载体，采取必要安全措施防止私钥遗失、泄露、篡改或被未经授权使用。
- 仅在证书有效期内，并在证书未被撤销、冻结或失效的情况下使用数字证书。
- 在发现私钥泄露、遗失、被盗用或存在其他安全风险时，及时向 GDCA 或相关注册机构申请证书撤销或冻结。
- 对其使用证书及私钥进行的电子签名行为承担相应责任。
- 配合 GDCA 完成证书申请、更新、撤销及其他相关业务办理。
- 遵守 GDCA 依法发布或更新的 CP/CPS、服务规范及安全管理要求。
- 如订户委托代理人办理证书业务，订户应确保代理行为合法有效，并对代理人在授权范围内的行为承担相应责任。

9.6.4. 依赖方的陈述与担保

依赖方在信赖 GDCA 签发的数字证书前，应合理审查和验证证书状态，并承担基于证书信赖行为产生的相应责任。依赖方承诺如下：

- 按照本 CP/CPS 及法律法规要求合理使用和信赖数字证书。
- 在信赖证书前，对证书信任链、证书有效期及证书用途等进行必要验证。
- 通过 CRL、OCSP 或其他有效方式确认数字证书状态。
- 根据证书用途、应用场景及安全风险，合理判断是否信赖相关数字证书。

- 不在证书失效、撤销、冻结或超出使用范围情况下信赖和使用数字证书。
- 遵守 GDCA 依法发布的 CP/CPS、服务规范及相关公告。
- 因依赖方未履行合理验证义务或超出合理信赖范围使用证书而造成的损失，由依赖方依法承担相应责任。

9.6.5. 其他参与者的陈述与担保

参与 GDCA 电子认证服务活动的其他相关参与方，应按照法律法规、主管部门要求及与 GDCA 签署的协议履行相应职责，并遵守本 CP/CPS 及安全管理要求。

9.7. 担保免责

除本 CP/CPS 第 9.6.1 节明确承诺的事项外，GDCA 不承担超出法律法规、本 CP/CPS、相关协议约定范围之外的其他担保责任。在法律法规允许范围内，GDCA 不对以下情形承担责任：

- 证书订户、依赖方或其他参与者提供信息不真实、不完整或存在误导所造成的损失；
- 因订户、依赖方或第三方未按照本 CP/CPS 要求使用、验证或信赖数字证书所造成的损失；
- 因数字证书超出规定用途、适用范围或有效期限使用所造成的损失；
- 因应用系统自身安全缺陷、网络故障、通信故障或第三方原因导致的损失；
- 因不可抗力事件，包括但不限于战争、自然灾害、重大疫情、电力中断、网络攻击等原因导致的服务中断、系统故障或数据损失；
- 因订户或依赖方违反本 CP/CPS、订户协议要求所造成的损失。

9.8. 偿付责任规则

GDCA 建立了电子认证服务偿付责任规则，用于规范因电子认证服务过程中可能产生的责任赔付及财务补偿机制。偿付责任范围涵盖 GDCA 在履行电子认证服务职责过程中，因技术故障、人为错误、安全漏洞、系统缺陷或管理失误等原因依法应承担责任的情形。

在不同责任情形下，GDCA 依据相关法律法规、主管部门要求、CP/CPS 及订户协议等，结合事件性质、过错责任比例及实际损失情况，确定相应赔付范围及赔付计算方

式。

GDCA 建立了赔付监督与管理机制，对赔付申请、责任认定、赔付执行及结果反馈进行全过程管理，并对相关处理过程进行记录与审计。

9.9. 赔偿

GDCA 建立了电子认证服务赔偿处理机制，用于规范因电子认证服务活动可能产生的赔偿申请、审核、审批及支付流程，并对各环节实施时限管理。赔偿流程包括申请受理、材料审核、责任认定、审批处理及赔付支付等环节，具体要求如下：

申请受理：GDCA 在收到赔偿申请及完整材料后，于 5 个工作日内完成受理确认，如材料不完整，应一次性告知补正要求。

审核与责任认定：自受理之日起，GDCA 应在 20 个工作日内完成事实核查与责任初步认定，对于复杂情况或需外部协查的，可适当延长。

审批处理：责任认定完成后，应在 10 个工作日内完成内部审批流程。

赔付支付：审批通过后，应在 10 个工作日内完成赔付支付，如涉及特殊支付方式或银行处理延迟，可相应顺延并说明原因。

如因客观原因导致无法在上述时限内完成处理，GDCA 应及时通知申请方，并说明延迟原因及预计完成时间。

9.10.有效期限与终止

9.10.1.有效期限

本 CP/CPS 自发布之日起生效，在未发布新版本或未被明确废止之前持续有效。GDCA 可根据法律法规、主管部门要求、业务发展或安全管理需要对本 CP/CPS 进行修订或更新，并按照规定流程发布新版本。

9.10.2.终止

当出现以下情形之一时，本 CP/CPS 全部或部分内容可被修订、替换或终止适用：

- 法律法规或主管部门相关规定发生变化，导致本 CP/CPS 部分或全部内容不再适用。
- 安全风险评估或审计结果表明相关条款不再符合安全要求。
- GDCA 发布新版本 CP/CPS 并明确替代原版本。

9.10.3.效力的终止与保留

对于电子认证服务参与者（包括订户、依赖方、注册机构或其他合作方），如其与 GDCA 之间的协议终止、合作关系结束或不再参与电子认证相关业务，则本 CP/CPS 中涉及其适用的相关条款自相应关系终止之日起不再对其继续适用，但不影响其在存续期间已产生的权利义务责任。

9.11.对参与者的个别通告与沟通

在电子认证服务活动中，GDCA 及相关参与方之间的通知、通告及业务沟通，应采用能够确保信息真实、完整、可追溯且在法律上可被认可的方式进行。

常用的有效通信方式包括但不限于：系统平台消息通知、电子邮件、短信通知、书面函件、在线业务系统公告以及经双方确认的其他电子化通信方式。

GDCA 在其业务系统或官方网站发布的公告、通知及业务规则更新信息，在符合相关约定的情况下，对相关参与方具有约束力。参与方应及时关注并按要求执行相关通知内容。

9.12.修订和发布

9.12.1.修订程序

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

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

9.12.2.CP/CPS 修订

GDCA 将对 CP/CPS 进行严格的版本控制，并由安全策略委员会负责相关事宜。

GDCA 根据国家的政策法规、技术要求、标准的变化及业务发展情况等及时修订本 CP/CPS。

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

本 CP/CPS 至少每年修订一次。修订后的 CP/CPS，从对外发布之日起三十日之内

向工业和信息化部备案。

9.12.3.通知机制和期限

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

9.12.4.必须修改 OID 的情形

GDCA 负责确定 CP/CPS 的修订是否需要修改 OID。

9.13.争议处理与举证

GDCA 建立了电子认证服务争议处理与举证机制，用于处理与 CP/CPS 及电子认证服务相关的争议事项。

争议处理范围包括但不限于证书申请、身份核验、证书签发、更新、撤销、冻结、电子签名、签名验证、证书状态服务及相关业务操作过程中产生的争议。相关参与方可通过客户服务渠道、书面申请或其他约定方式提出争议处理申请。GDCA 收到申请后，应按照内部流程进行受理、核查、处理及反馈，并自正式受理之日起 10 个工作日内组织争议相关方开展协商处理，对于情况复杂、涉及重大安全事件或需第三方协查的争议事项，协商处理期限可适当延长，并应及时告知相关方延长原因及预计完成时间。协商无法达成一致的，可依法通过调解、仲裁或诉讼等方式解决。双方另有约定的，从其约定。涉及诉讼或仲裁的，按照相关法律法规及协议约定确定管辖及适用规则。

GDCA 建立覆盖证书全生命周期的举证与证据保全体系，包括但不限于：

- 证书签发环节的身份验证记录、申请资料、审核记录、告知记录、意愿确认记录及协议签署记录；
- 电子签名环节的签名请求验证记录、签名操作日志、授权记录、时间戳记录及相关审计信息；
- 签名验证环节的验证请求记录、验证结果记录、异常处理记录及相关日志信息；
- 证书更新、冻结、撤销及状态查询等相关业务记录。

上述记录和日志应按照法律法规、主管部门要求及 GDCA 相关管理制度进行保存，并采取防篡改保护措施。

对于依法有权获取相关举证材料的主体，GDCA 在完成身份核验及合法性审核后，

应按照规定流程提供相关材料。一般情况下，GDCA 应自正式受理申请之日起 10 个工作日内完成举证材料的整理与提供，情况复杂或涉及外部协查的，可适当延长，并告知申请方相关情况。

9.14.管辖法律

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

9.15.与适用法律的符合性

GDCA 及电子认证服务相关参与方在开展电子认证服务活动过程中，应遵守中华人民共和国现行有效的法律法规、部门规章、规范性文件及相关国家标准要求。

适用的法律法规包括但不限于：《中华人民共和国电子签名法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《商用密码管理条例》、《电子认证服务管理办法》、《电子认证服务密码管理办法》、《电子认证业务规则规范》以及其他与电子认证服务、网络安全、数据安全、个人信息保护和商用密码管理相关的法律法规及主管部门要求。

9.16.一般条款

9.16.1.完整协议

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

GDCA 的 CP/CPS 由标题、目录、正文构成。本 CP/CPS 自正式发布之日起生效，并替代 GDCA 此前发布的同类认证业务规则文件。

GDCA 将在官方网站发布现行有效版本的 CP/CPS，供相关参与方查阅和使用。订户协议、依赖方协议及相关业务协议中应明确所对应适用的 CP/CPS 版本信息。

9.16.2.转让

GDCA 声明，根据本 CP/CPS 中详述的认证实体各方的权利和义务，各方当事人可按照法律的相关规定进行权利和义务的转让。此类转让不影响转让方在转让前已经产生

的责任和义务。

9.16.3.分割性

如果本 CP/CPS 的任何条款或其适用因与适用法律法规发生冲突而被认定为无效、违法或不可执行，GDCA 可在必要范围内对相关条款进行修订，使其在最大程度上保持有效和可执行。本 CP/CPS 其余条款不受影响，并继续保持有效。

若相关法律法规或监管要求发生变化，GDCA 可依据实际情况对本 CP/CPS 进行相应调整。

9.16.4.强制执行（律师费用和权利放弃）

GDCA 声明,若证书订户、依赖方或其他参与方严格履行本 CP/CPS 中的某项规定，不应被视为对该项权利或其他权利的放弃，也不影响 GDCA 在后续要求相关方继续履行相应义务。

9.16.5.不可抗力

对于因不可抗力事件导致 GDCA 无法履行或延迟履行本 CP/CPS 项下义务的，GDCA 不承担相应责任。不可抗力包括但不限于战争、重大公共卫生事件、自然灾害、重大网络攻击、电力或通信基础设施故障以及其他无法预见、无法避免且无法克服的事件。

9.17.其他条款

GDCA 对本 CP/CPS 具有最终解释权。