

数安时代科技股份有限公司

SSL/TLS 证书策略及电子认证业务规则

版本：1.0

发布日期：2026 年 10 月 31 日

Global Digital Cybersecurity Authority CO., LTD.

SSL/TLS Certificate Policy and Certification Practice Statement

Version: 1.0

Release Date: October 31, 2026

目录

Contents

1. 概括性描述 Introduction 1

1.1. 概述 Overview 1

1.1.1 公司简介 Company Profile 1

1.1.2 证书策略与电子认证业务规则（CP/CPS） 1

1.1.3 GDCA 证书层次架构 GDCA Certificate Hierarchical Architecture 3

1.2. 文档名称与标识 Document Name and Identification 4

1.2.1. 修订历史 Revisions 4

1.3. PKI 参与者 PKI Participants 4

1.3.1. 电子认证服务机构 Certification Authorities 4

1.3.2. 订户 Subscribers 5

1.3.3. 依赖方 Relying Parties 5

1.3.4. 其他参与者 Other Participants 5

1.4. 证书应用 Certificate Usage 5

1.5. 策略管理 Policy Administration 6

1.5.1 策略文档管理机构 Organization Administering the Document 7

1.5.2 联系人 Contact Person 7

1.5.3 决定 CPS 符合策略的机构 Person Determining CPS Suitability for the Policy 8

1.5.4 CP/CPS 批准程序 CPS Approval Procedures 8

1.5.5 CP/CPS 修订 CPS Revision 8

1.6. 定义和缩写 Definitions and Acronyms 9

1.6.1 术语定义一览表 List of Term Definition 9

1.6.2 缩略语及其含义一览表 List of Abbreviations and their Meaning 11

2. 信息发布与信息管理 Publication and Repository Responsibilities 12

2.1. GDCA 信息库 Repositories 12

2.2. 信息的发布 Publication of Certification Information 12

2.3. 发布的时间和频率 Time or Frequency of Publication 13

2.4. 信息库访问控制 Access Controls on Repositories 13

3. 身份标识与鉴别 Identification and Authentication 14
3.1. 命名 Naming 14
3.1.1. 名称类型 Types of Names 14
3.1.2. 对名称意义化的要求 Need for Names to be Meaningful 14
3.1.3. 订户的匿名或伪名 Anonymity or Pseudonymity of Subscribers 14
3.1.4. 理解不同名称的形式的规则 Rules for Interpreting Various Name Forms ... 14
3.1.5. 名称的唯一性 Uniqueness of Names 15
3.1.6. 商标的识别、鉴别与角色 Recognition, Authentication, and Role of Trademarks 15
3.2. 初始身份确认 Initial Identity Validation 15
3.2.1. 证明拥有私钥的方法 Method to Prove Possession of Private Key 15
3.2.2. 机构身份和域名的鉴别 Authentication of Organization and Domain Identity 15
3.2.3. 个人身份的鉴别 Authentication of Individual Identity 34
3.2.4. 没有验证的订户信息 Non-Verified Subscriber Information 34
3.2.5. 授权确认 Validation of Authority 34
3.2.6. 互操作准则 Criteria for Interoperation 35
3.3. 密钥更新请求的标识与鉴别 Identification and Authentication for Re-key Requests 35
3.3.1 常规密钥的更新的标识与鉴别 Identification and Authentication for Routine Re-key 36
3.3.2 撤销后密钥更新的标识与鉴别 Identification and Authentication for Re-key After Revocation 36
3.4. 撤销请求的标识与鉴别 Identification and Authentication for Revocation Request 36
3.5. 授权服务机构的标识和鉴别 Identification and Authentication for Authorized Service Organization 37
4. 证书生命周期操作要求 Certificate Life Cycle Operational Requirements 37
4.1. 证书申请 Certificate Application 37
4.1.1. 证书申请实体 Who Can Submit a Certificate Application 37
4.1.2. 注册过程与责任 Enrollment Process and Responsibilities 37
4.2. 证书申请处理 Certificate Application Processing 38

4.2.1. 识别与鉴别功能 Performing Identification and Authentication Functions 38
4.2.2. 证书申请批准和拒绝 Approval or Rejection of Certificate Applications 39
4.2.3. 处理证书申请的时间 Time to Process Certificate Applications 40
4.2.4. 认证机构授权（CAA）Certification Authority Authorization (CAA) 41
4.3. 证书签发 Certificate Issuance 42
4.3.1. 证书签发过程中注册机构（RA）和电子认证服务机构（CA）的行为 CA Actions During Certificate Issuance 42
4.3.2. 电子认证服务机构和注册机构对订户的通告 Notifications to Subscriber by the CA of Issuance of Certificate 43
4.4. 证书接受 Certificate Acceptance 43
4.4.1. 构成接受证书的行为 Conduct Constituting Certificate Acceptance 43
4.4.2. 电子认证服务机构对证书的发布 Publication of the Certificate by the CA .. 44
4.4.3. 电子认证服务机构对其他实体的通告 Notification of Certificate Issuance by the CA to Other Entities 44
4.5. 密钥对和证书的使用 Key Pair and Certificate Usage 44
4.5.1. 订户的私钥和证书的使用 Subscriber Private Key and Certificate Usage 44
4.5.2. 依赖方公钥和证书的使用 Relying Party Public Key and Certificate Usage . 45
4.6. 证书更新 Certificate Renewal 45
4.6.1. 证书更新的情形 Circumstances for Certificate Renewal 45
4.6.2. 请求证书更新的实体 Who May Request Renewal 45
4.6.3. 证书更新请求的处理 Processing Certificate Renewal Requests 45
4.6.4. 颁发新证书时对订户的通告 Notification of New Certificate Issuance to Subscriber 46
4.6.5. 构成接受更新证书的行为 Conduct Constituting Acceptance of a Renewal Certificate 46
4.6.6. 电子认证服务机构对更新证书的发布 Publication of the Renewal Certificate by the CA 46
4.6.7. 电子认证服务机构对其他实体的通告 Notification of Certificate Issuance by the CA to Other Entities 46
4.7. 证书密钥更新 Certificate Rekey 46
4.7.1. 证书密钥更新的情形 Circumstances for Certificate Rekey 46

4.7.2. 请求证书密钥更新的实体 Who May Request Certification of a New Public Key 47
4.7.3. 证书密钥更新请求的处理 Processing Certificate Rekeying Requests 47
4.7.4. 颁发新证书时对订户的通告 Notification of New Certificate Issuance to Subscriber 47
4.7.5. 构成接受密钥更新证书的行为 Conduct Constituting Acceptance of a Rekeyed Certificate 47
4.7.6. 电子认证服务机构对密钥更新证书的发布 Publication of the Rekeyed Certificate by the CA 47
4.7.7. 电子认证服务机构对其他实体的通告 Notification of Certificate Issuance by the CA to Other Entities 47
4.8. 证书变更 Certificate Modification 48
4.8.1. 证书变更的情形 Circumstances for Certificate Modification 48
4.8.2. 请求证书变更的实体 Who May Request Certificate Modification 48
4.8.3. 证书变更请求的处理 Processing Certificate Modification Requests 48
4.8.4. 颁发新证书时对订户的通告 Notification of New Certificate Issuance to Subscriber 48
4.8.5. 构成接受变更证书的行为 Conduct Constituting Acceptance of Modified Certificate 48
4.8.6. 电子认证服务机构对变更证书的发布 Publication of the Modified Certificate by the CA 48
4.8.7. 电子认证服务机构对其他实体的通告 Notification of Certificate Issuance by the CA to Other Entities 49
4.9. 证书撤销和挂起 Certificate Revocation and Suspension 49
4.9.1. 证书撤销的情形 Circumstances for Revocation 49
4.9.2. 请求证书撤销的实体 Who Can Request Revocation 52
4.9.3. 撤销请求的流程 Procedure for Revocation Request 53
4.9.4. 撤销请求宽限期 Revocation Request Grace Period 55
4.9.5. 电子认证服务机构处理撤销请求的时限 Time Within Which CA Must Process the Revocation Request 55
4.9.6. 依赖方检查证书撤销的要求 Revocation Checking Requirements for Relying Parties 55

4.9.7. CRL 发布频率 CRL Issuance Frequency 55
4.9.8. CRL 发布的最大滞后时间 Maximum Latency for CRLs 55
4.9.9. 在线状态查询的可用性 Online Revocation/Status Checking Availability 56
4.9.10. 在线状态查询要求 Online Revocation Checking Requirements 56
4.9.11. 撤销信息的其他发布形式 Other Forms of Revocation Advertisements Available 56
4.9.12. 密钥损害的特别要求 Special Requirements related to Key Compromise 57
4.9.13. 证书挂起的情形 Circumstances for Suspension 57
4.9.14. 请求证书挂起的实体 Who Can Request Suspension 57
4.9.15. 挂起请求的流程 Procedure for Suspension Request 58
4.9.16. 挂起的期限限制 Limits on Suspension Period 58
4.10. 证书状态服务 Certificate Status Services 58
4.10.1. 操作特征 Operational Characteristics 58
4.10.2. 服务可用性 Service Availability 58
4.10.3. 可选特征 Operational Features 58
4.11. 订购结束 End of Subscription 59
4.12. 密钥生成、备份与恢复 Key Escrow and Recovery 59
4.12.1. 密钥生成、备份与恢复的策略与行为 Key Escrow and Recovery Policy and Practices 60
4.12.2. 会话密钥的封装与恢复的策略和行为 Session Key Encapsulation and Recovery Policy and Practices 60
5. 认证机构设施、管理和操作控制 Facility, Management, and Operational Controls 60
5.1. 物理控制 Physical Controls 60
5.1.1. 场地位置与建筑 Site Location and Construction 60
5.1.2. 物理访问 Physical Access 62
5.1.3. 安防监控 Security Monitoring 63
5.1.4. 电力与空调 Power and Air Conditioning 64
5.1.5. 水患防治 Water Exposures 64
5.1.6. 火灾防护 Fire Prevention and Protection 65
5.1.7. 介质存储 Media Storage 65
5.1.8. 废物处理 Waste Disposal 66

5.1.9. 异地备份 Off-Site Backup 66
5.2. 程序控制 Procedural Controls 66
5.2.1. 可信角色 Trusted Roles 66
5.2.2. 每项任务需要的角色 Number of Persons Required per Task 67
5.2.3. 每个角色的识别与鉴别 Identification and Authentication for Each Role 67
5.2.4. 需要职责分割的角色 Roles Requiring Separation of Duties 67
5.3. 人员控制 Personnel Controls 68
5.3.1. 资格、经历和无过失要求 Qualifications, Experience, and Clearance Requirements 68
5.3.2. 背景审查程序 Background Check Procedures 69
5.3.3. 培训要求 Training Requirements 70
5.3.4. 再培训周期和要求 Retraining Frequency and Requirements 71
5.3.5. 工作岗位轮换周期和顺序 Job Rotation Frequency and Sequence 72
5.3.6. 未授权行为的处罚 Sanctions for Unauthorized Actions 72
5.3.7. 独立合约人的要求 Independent Contractor Requirements 72
5.3.8. 提供员工的文档 Documentation supplied to Personnel 72
5.4. 审计日志程序 Audit Logging Procedures 73
5.4.1. 记录事件的类型 Types of Event recorded 73
5.4.2. 处理日志的周期 Frequency of Processing Log 74
5.4.3. 审计日志的保存期限 Retention Period for Audit Log 75
5.4.4. 审计日志的保护 Protection of Audit Log 75
5.4.5. 审计日志备份程序 Audit Log Backup Procedures 75
5.4.6. 审计收集系统 Audit Collection System 75
5.4.7. 对导致事件实体的通告 Notification to Event-Causing Subject 76
5.4.8. 脆弱性评估 Vulnerability Assessments 76
5.5. 记录归档 Records Archival 77
5.5.1. 归档记录的类型 Types of Records Archived 77
5.5.2. 归档记录的保存期限 Retention Period for Archive 77
5.5.3. 归档文件的保护 Protection of Archive 77
5.5.4. 归档文件的备份程序 Archive Backup Procedures 77

5.5.5. 记录时间戳要求 Requirements for Time-Stamping of Records 78
5.5.6. 归档收集系统 Archives Collection System 78
5.5.7. 获得和检验归档信息的程序 Procedures to Obtain and Verify Archive Information 78
5.6. 电子认证服务机构密钥的更替 Key Changeover 78
5.7. 损害与灾难恢复 Compromise and Disaster Recovery 79
5.7.1. 事故和损害处理程序 Incident and Compromise Handling Procedures 79
5.7.2. 计算资源、软件和或/数据的损坏 Computing Resources, Software, and/or Data Are Corrupted 80
5.7.3. 实体私钥损害处理程序 Entity Private Key Compromise Procedures 80
5.7.4. 灾难后的业务连续性能力 Business Continuity Capabilities After a Disaster 82
5.8. 电子认证服务机构或注册机构的终止 CA or RA Termination 82
6. 认证系统技术安全控制 Technical Security Controls 84
6.1. 密钥对的生成与安装 Key Pair Generation and Installation 84
6.1.1. 密钥对的生成 Key Pair Generation 84
6.1.2. 私钥传送给订户 Private Key Delivery to Subscriber 85
6.1.3. 公钥传送给证书签发机构 Public Key Delivery to Certificate Issuer 85
6.1.4. 电子认证服务机构公钥传送给依赖方 CA Public Key Delivery to Relying Parties 85
6.1.5. 密钥的长度 Key Sizes 86
6.1.6. 公钥参数的生成和质量检查 Public Key Parameters Generation and Quality Checking 86
6.1.7. 密钥使用目的（基于 X.509 v3 密钥用途字段）Key Usage Purposes (as per X.509 v3 Key Usage Field) 86
6.2. 私钥保护和密码模块工程控制 Private Key Protection and Cryptographic Module Engineering Controls 86
6.2.1. 密码模块的标准和控制 Cryptographic Module Standards and Controls 86
6.2.2. 私钥多人控制（m 选 n）Private Key (n out of m) Multi-Person Control 87
6.2.3. 私钥托管 Private Key Escrow 87
6.2.4. 私钥备份 Private Key Backup 87
6.2.5. 私钥归档 Private Key Archival 87

6.2.6. 私钥导出、导入密码模块 Private Key Transfer Into or From a Cryptographic Module 87
6.2.7. 私钥在密码模块的存储 Private Key Storage on Cryptographic Module..... 88
6.2.8. 激活私钥的方法 Methods of Activating Private Key 88
6.2.9. 解除私钥激活状态的方法 Method of Deactivating Private Key 88
6.2.10. 销毁私钥的方法 Method of Destroying Private Key..... 89
6.2.11. 密码模块的评估 Cryptographic Module Rating 89
6.3. 密钥对管理的其他方面 Other Aspects of Key Pair Management 89
6.3.1. 公钥归档 Public Key Archival 89
6.3.2. 证书操作期和密钥对使用期限 Certificate Operational Periods and Key Pair Usage Periods..... 89
6.4. 激活数据 Activation Data..... 90
6.4.1. 激活数据的产生和安装 Activation Data Generation and Installation 90
6.4.2. 激活数据的保护 Activation Data Protection 90
6.4.3. 激活数据的其他方面 Other Aspects of Activation Data..... 91
6.5. 计算机安全控制 Computer Security Controls 91
6.5.1. 特别的计算机安全技术要求 Specific Computer Security Technical Requirements..... 91
6.5.2. 计算机安全评估 Computer Security Rating 92
6.6. 生命周期技术控制 Life Cycle Technical Controls..... 93
6.6.1. 系统开发控制 System Development Controls 93
6.6.2. 安全管理控制 Security Management Controls 93
6.6.3. 生命周期的安全控制 Life Cycle Security Controls 94
6.7. 网络的安全控制 Network Security Controls 94
6.8. 时间戳 Time-Stamping 95
7. 证书、证书撤销列表和在线证书状态协议 Certificate, CRL, and OCSP Profiles 95
7.1. 证书 Certificate Profile 95
7.1.1. 版本号 Version Number(s) 97
7.1.2. 证书扩展项 Certificate Extensions..... 97
7.1.3. 算法对象标识符 Algorithm Object Identifiers..... 103
7.1.4. 名称形式 Name Forms 103

7.1.5. 名称限制 Name Constraints 104
7.1.6. 证书策略对象标识符 Certificate Policy Object Identifier 104
7.1.7. 策略限制扩展项的用法 Usage of Policy Constraints Extension 104
7.1.8. 策略限定符的语法和语义 Policy Qualifiers Syntax and Semantics 104
7.1.9. 关键证书策略扩展项的处理规则 Processing Semantics for the Critical Certificate Policies Extension 104
7.2. 证书撤销列表 CRL Profile 104
7.2.1. 版本 Version Number(s) 104
7.2.2. CRL 和 CRL 条目扩展项 CRL and CRL Entry Extensions 105
7.3. 在线证书状态协议 OCSP Profile 106
7.3.1. 版本号 Version Number(s) 106
7.3.2. OCSP 扩展项 OCSP Extensions 106
8. 认证机构审计和其他评估 Compliance Audit and Other Assessments 107
8.1. 评估的频率或情形 Frequency or Circumstances of Assessment 107
8.2. 评估者的身份/资质 Identity/Qualifications of Assessor 107
8.3. 评估者与被评估者之间的关系 Assessor’s Relationship to Assessed Entity 108
8.4. 评估内容 Topics Covered by Assessments 108
8.5. 对问题与不足采取的措施 Actions Taken as a Result of Deficiency 109
8.6. 评估结果的传达与发布 Communications of Results 109
8.7. 自评估 Self-Audits 109
9. 法律责任和其他业务条款 Other Business and Legal Matters 110
9.1. 费用 Fees 110
9.1.1. 证书签发和更新 Certificate Issuance and Renewal Fees 110
9.1.2. 证书查询费用 Certificate Access Fees 110
9.1.3. 证书撤销或状态信息的查询费用 Revocation or Status Information Access Fees 110
9.1.4. 其他服务费用 Fees for Other Services 111
9.1.5. 退款策略 Refund Policy 111
9.2. 财务责任 Financial Responsibility 112
9.2.1. 保险范围 Insurance Coverage 112

9.2.2. 其他资产 Other Assets 112
9.2.3. 对最终实体的保险或担保 Insurance or Warranty Coverage for End-Entities 112
9.3. 业务信息保密 Confidentiality of Business Information 112
9.3.1. 保密信息范围 Scope of Confidential Information 112
9.3.2. 不属于保密的信息 Information Not Within the Scope of Confidential Information 113
9.3.3. 保护保密信息的责任 Responsibility to Protect Confidential Information 113
9.4. 个人隐私保密 Privacy of Personal Information 114
9.4.1. 隐私保密方案 Privacy Plan 114
9.4.2. 作为隐私处理的信息 Information Treated as Private 114
9.4.3. 不被视为隐私的信息 Information Not Deemed Private 114
9.4.4. 保护隐私的责任 Responsibility to Protect Private Information 115
9.4.5. 使用隐私信息的告知与同意 Notice and Consent to Use Private Information 115
9.4.6. 依法律或行政程序的信息披露 Disclosure Pursuant to Judicial or Administrative Process 115
9.4.7. 其他信息披露情形 Other Information Disclosure Circumstances 116
9.5. 知识产权 Intellectual Property Rights 116
9.6. 陈述与担保 Representations and Warranties 116
9.6.1. 电子认证服务机构的陈述与担保 CA Representations and Warranties 116
9.6.2. 注册机构的陈述与担保 RA Representations and Warranties 118
9.6.3. 订户的陈述与担保 Subscriber Representations and Warranties 118
9.6.4. 依赖方的陈述与担保 Representations and Warranties of Relying Party 120
9.6.5. 其他参与者的陈述与担保 Representations and Warranties of Other Participants 121
9.7. 担保免责 Disclaimers of Warranties 121
9.8. 有限责任 Limitations of Liability 121
9.9. 赔偿 Indemnities 122
9.9.1. GDCA 的赔偿责任 Indemnification by GDCA 122
9.9.2. 订户的赔偿责任 Indemnification by Subscribers 123

9.9.3. 依赖方的赔偿责任 Indemnification by Relying Parties 124
9.10. 有效期限与终止 Term and Termination 125
9.10.1. 有效期限 Term..... 125
9.10.2. 终止 Termination 125
9.10.3. 效力的终止与保留 Effect of Termination and Survival 125
9.11. 对参与者的个别通告与沟通 Individual Notices and Communications with Participants126
9.12. 修订 Amendments..... 126
9.12.1. 修订程序 Procedures for Amendment 126
9.12.2. 通知机制和期限 Notification Mechanism and Periods..... 126
9.12.3. 必须修改 OID 的情形 Circumstances under which OID Must be Changed. 127
9.13. 争议处理 Dispute Resolution Provisions..... 127
9.14. 管辖法律 Governing Law 127
9.15. 与适用法律的符合性 Compliance with Applicable Law 127
9.16. 一般条款 Miscellaneous Provisions 128
9.16.1. 完整协议 Entire Agreement..... 128
9.16.2. 转让 Assignment 128
9.16.3. 分割性 Severability 128
9.16.4. 强制执行（律师费用和权利放弃）Enforcement (Attorneys' Fees and Waiver of Rights) 129
9.16.5. 不可抗力 Force Majeure..... 129
9.17. 其他条款 Other Provisions 129

1. 概括性描述 Introduction

1.1. 概述 Overview

1.1.1 公司简介 Company Profile

数安时代科技股份有限公司（Global Digital Cybersecurity Authority Co., Ltd.，简称 GDCA 或“数安时代”），原为“广东数字证书认证中心有限公司”，成立于 2003 年 3 月 6 日。2005 年 9 月，GDCA 依法通过了国家密码管理局和原国家信息产业部的资格审查，成为全国首批八家获得《电子认证服务许可证》（许可证号：ECP44010220007）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。为适应业务发展需要，2016 年 5 月，“广东数字证书认证中心有限公司”更名为“数安时代科技股份有限公司”。2017 年 8 月 11 日，GDCA 在新三板挂牌交易，股票简称：数安时代，股票代码：871932。

Global Digital Cybersecurity Authority Co., Ltd. (abbreviated as GDCA or “数安时代”), formerly known as Guang Dong Certificate Authority Co., Ltd., was established on March 6, 2003. In September 2005, GDCA passed the qualification review of the State Cryptography Administration (SCA) and the former Ministry of Information Industry, becoming one of the first eight electronic certification service providers nationwide to obtain the Electronic Certification Service License (License No.: ECP44010220007). In December 2008, GDCA obtained the Commercial Cryptography Product Sales License issued by the SCA. In April 2011, GDCA passed the e-Government electronic certification service capability assessment organized by the SCA and obtained the qualification of e-Government Electronic Certification Service Provider (No.: A021). In 2013, GDCA upgraded its electronic certification service system with the SM2 algorithm and passed the security review organized by the SCA. In 2015, GDCA obtained WebTrust international security audit certification. To meet business development needs, the company was renamed Global Digital Cybersecurity Authority Co., Ltd. in May 2016, replacing its former name Guang Dong Certificate Authority Co.,Ltd. On August 11, 2017, GDCA was listed on the National Equities Exchange and Quotations (NEEQ), with the stock abbreviation “数安时代” and stock code 871932.

1.1.2 证书策略与电子认证业务规则（CP/CPS）

本证书策略与电子认证业务规则（简称 CP/CPS）详细阐述了 GDCA 提供的电子认证服务整个过程、电子认证服务所遵循的规则以及电子认证服务相关参与者所承担的责任。本 CP/CPS 由 GDCA 通过公开发布的形式告知订户、依赖方和其他相关参与者。

本 CP/CPS 适用于根据以下最新版本的策略、指南和标准所签发的 SSL/TLS 服务器证书：

- CA/B Forum 公共可信证书签发与管理基础要求（TLS BRs）；
- CA/B Forum 扩展验证（EV）证书指南（EVGs）；
- CA/B Forum 网络与证书系统安全要求（NCSSRs）；
- Microsoft 可信根证库计划要求；
- 360 浏览器 CA 策略要求；
- Mozilla 根证书库策略要求；
- Apple 根证书库计划要求；
- Chrome 根证书库计划要求；
- 通用认证机构数据库（CCADB）策略要求。

This CP/CPS provides a detailed description of the entire process of electronic certification services provided by GDCA, the rules governing such services, and the responsibilities borne by subscribers, relying parties, and other participants involved in electronic certification services. This CP/CPS is made available to subscribers, relying parties, and other relevant participants through public disclosure by GDCA.

This CP/CPS governs the SSL/TLS server certificates issued under the following latest policies, guidelines and standards:

- The CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (“TLS BRs”);
- The CA/B Forum Guidelines for Extended Validation Certificates (“EVGs”);
- The CA/B Forum Network and Certificate System Security Requirements(“NCSSRs”);
- Microsoft Trusted Root Program Requirements;
- 360 Browser CA Policy;
- Mozilla Root Store Policy;
- Apple Root Store Program;
- Chrome Root Program Policy;
- Common Certification Authority Database (CCADB) Policy.

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

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CP/CPS is divided into nine parts that cover the security controls and practices and procedures for GDCA’s certificate services. To

preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement “Not applicable”.

1.1.3 GDCA 证书层次架构 GDCA Certificate Hierarchical Architecture

GDCA 目前有 3 个根证书用于签发 SSL/TLS 服务器证书，分别为 GDCA TrustAUTH R5 ROOT、GDCA TLS ROOT R52、及 GDCA TLS ROOT E52。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。

GDCA 根证书信息：

（1）GDCA TrustAUTH R5 ROOT

SHA256 指纹：

BFFF8FD04433487D6A8AA60C1A29767A9FC2BBB05E420F713A13B992891D3893

（2）GDCA TLS ROOT R52

SHA256 指纹：

77AE39E8D124F6BC747C74FA8DA2AE089358C4930566ED7369144672D74C6471

（3）GDCA TLS ROOT E52

SHA256 指纹：

D50FDF57D3CEC20EE91256A4A6DA768C36A510DFE5771F23EF4B1833290BF012

GDCA 根证书及中级 CA 证书通过 GDCA 网站（https://www.gdca.com.cn）发布。

GDCA currently operates three root certificates for issuing SSL/TLS server certificates, namely GDCA TrustAUTH R5 ROOT, GDCA TLS ROOT R52, and GDCA TLS ROOT E52. Each root CA contains subordinate CA certificates for the issuance of end-entity certificates. GDCA does not issue externally operated subordinate CA certificates.

GDCA Root Certificate Information:

(1) GDCA TrustAUTH R5 ROOT

SHA-256 Fingerprint:

BFFF8FD04433487D6A8AA60C1A29767A9FC2BBB05E420F713A13B992891D3893

(2) GDCA TLS ROOT R52

SHA-256 Fingerprint:

77AE39E8D124F6BC747C74FA8DA2AE089358C4930566ED7369144672D74C6471

(3) GDCA TLS ROOT E52

SHA-256 Fingerprint:

D50FDF57D3CEC20EE91256A4A6DA768C36A510DFE5771F23EF4B1833290BF012

GDCA root certificates and subordinate CA certificates are published on the GDCA website

(https://www.gdca.com.cn).

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

本文档称作《数安时代科技股份有限公司 SSL/TLS 证书策略及电子认证业务规则》（简称 GDCA CP/CPS、本 CP/CPS）。本 CP/CPS 以中英文双语形式发布，GDCA 应确保英文版本与中文版本无重大不一致的地方。

This document is titled the “GDCA SSL/TLS Certificate Policy and Certification Practice Statement” (abbreviated as GDCA CP/CPS or this CP/CPS). This CP/CPS is published in both Chinese and English, and GDCA should make sure that there are no material differences between the Chinese and English version.

1.2.1. 修订历史 Revisions

日期	修订内容	版本号
2026.10.31	本版本将 SSL/TLS 证书业务相关的证书策略（CP）与认证业务规则（CPS）整合为一份独立的 CP/CPS 文档，并作为新的版本发布。历史版本内容可参阅相关历史文档。	1.0

Date	Revisions	Version
2026.10.31	This version consolidates the Certificate Policy (CP) and Certification Practice Statement (CPS) related to SSL/TLS certificate services into a standalone CP/CPS document and formally releases it as a new version. Previous versions may be referenced in the historical documentation.	1.0

1.3. PKI 参与者 PKI Participants

1.3.1. 电子认证服务机构 Certification Authorities

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

GDCA is a publicly trusted third-party electronic certification service provider established in accordance with the Electronic Signature Law of the People’s Republic of China and the Administrative Measures for Electronic Certification Services. By issuing digital certificates to parties engaged in electronic transactions and providing certificate validation services, GDCA serves as a participating entity in electronic certification activities.

1.3.2. 订户 Subscribers

订户指从 GDCA 接收数字证书的实体，可以是个人、机构、或设备。订户通常需要同 GDCA 签订合约以获得证书，并承担作为证书订户的责任。

A subscriber refers to an entity that receives a digital certificate from GDCA, and may be an individual, an organization, or a device. Subscribers typically must enter into an agreement with GDCA to obtain a certificate and assume the responsibilities as a certificate subscriber.

1.3.3. 依赖方 Relying Parties

GDCA 的证书依赖方是指基于对 GDCA 签发的证书及有关数字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。

A relying party of GDCA refers to an entity that engages in relevant activities based on its trust in the certificates issued by GDCA and the associated digital signatures. Such an entity may or may not be a subscriber of GDCA.

1.3.4. 其他参与者 Other Participants

其他参与者是指为 GDCA 的电子认证活动提供相关服务的其他实体。

Other participants refer to entities that provide relevant services for GDCA's electronic certification activities.

1.4. 证书应用 Certificate Usage

1.4.1.1. 适合的证书应用 Appropriate Certificate Usage

GDCA 签发的 SSL/TLS 服务器证书标识 Web 网站或者 Web 服务器的身份，可以用于证明网站的身份、提供 SSL 加密通道。SSL/TLS 服务器类证书又分为 DV SSL（Domain Validation SSL）证书、OV SSL（Organization Validation SSL）证书和 EV SSL（Extended Validation SSL）证书。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。

SSL/TLS server certificates issued by GDCA identify the identity of a website or web server, and can be used to prove the website's identity, as well as to provide an SSL-encrypted communication channel. SSL/TLS server certificates are further categorized into DV SSL (Domain Validation SSL) certificates, OV SSL (Organization Validation SSL) certificates, and EV SSL (Extended Validation SSL) certificates. Subscribers may determine and select the appropriate certificate type based on their actual needs.

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

证书类别	策略对象标识符	密钥用法
DV SSL 证书	1.2.156.112559.1.1.4.3 及 2.23.140.1.2.1	密钥用法：数字签名，密钥加密。 增强型密钥用法：服务器身份验证。
OV SSL 证书	1.2.156.112559.1.1.4.1 及 2.23.140.1.2.2	密钥用法：数字签名，密钥加密。 增强型密钥用法：服务器身份验证。
EV SSL 证书	1.2.156.112559.1.1.6.1 及 2.23.140.1.1	密钥用法：数字签名，密钥加密。 增强型密钥用法：服务器身份验证。

Types of Certificates	Policy OIDs	Key Usages
DV SSL Certificates	1.2.156.112559.1.1.4.3 and 2.23.140.1.2.1	KU: Digital Signature, Key Encipherment. EKU: Server Authentication.
OV SSL Certificates	1.2.156.112559.1.1.4.1 and 2.23.140.1.2.2	KU: Digital Signature, Key Encipherment. EKU: Server Authentication.
EV SSL Certificates	1.2.156.112559.1.1.6.1 and 2.23.140.1.1	KU: Digital Signature, Key Encipherment. EKU: Server Authentication.

1.4.1.3. 限制的证书应用 Prohibited Certificate Uses

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

The use of certificates issued by GDCA is prohibited in any circumstances that violate national laws or regulations or jeopardize national security. The use of certificates in any illegal or criminal activities or in business activities prohibited by law is also strictly forbidden. The subscriber shall bear all legal consequences arising from any such misuse.

1.5. 策略管理 Policy Administration

GDCA 安全策略委员会是 GDCA 电子认证服务所有策略的最高管理机构，负责审核批准 CP/CPS。

The GDCA Security Policy Committee is the highest governing body for all policies related to GDCA's electronic certification services and is responsible for reviewing and approving the CP/CPS.

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

策略文档管理机构为 GDCA 安全策略委员会，作为策略管理机构负责制订、发布、更新本 CP/CPS。GDCA 安全策略委员会由来自于公司管理层、行政中心、技术中心、运营服务中心等拥有决策权的合适代表组成。

The policy document management body is the GDCA Security Policy Committee, which, as the policy management authority, is responsible for formulating, publishing, and updating this CP/CPS. The GDCA Security Policy Committee is composed of appropriate representatives with decision-making authority from the company's management, administrative center, technical center, and operations service center etc.

1.5.2 联系人 Contact Person

1.5.2.1. 证书问题报告 Certificate Problem Report

证书问题报告及证书撤销请求须通过以下方式之一提交，且证书撤销请求必须以书面形式提交：

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

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

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

1.5.2.2. CP/CPS 问题 CP/CPS Related Issues

任何有关 CP/CPS 的问题、建议、疑问等，都可以按以下方式进行联系。

联系部门：GDCA 行政管理部门

网站地址：https://www.gdca.com.cn/

电子邮箱地址：gdca@gdca.com.cn

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

邮政编码：510030

电话号码：+86 20-83487228

Any questions, suggestions, or inquiries regarding this CP/CPS may be directed to the following contact:

Contact Department: GDCA Administrative Department

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

E-mail: gdca@gdca.com.cn

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

Postal Code: 510030

Tel: +86 20-83487228

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

GDCA 安全策略委员会负责确定本文件的适用性和适用范围。

The GDCA Security Policy Committee determines the suitability and applicability of this document.

1.5.4 CP/CPS 批准程序 CPS Approval Procedures

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。

The GDCA CP/CPS is drafted by the CP/CPS drafting team organized by the GDCA Security Policy Committee. Upon completion, the draft is submitted to the GDCA Security Policy Committee for review. After approval by the committee, the CP/CPS will be officially published on the GDCA official website.

1.5.5 CP/CPS 修订 CPS Revision

GDCA 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。

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

GDCA implements strict version control over the CP/CPS, with the Security Policy Committee responsible for all related matters.

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

1.6. 定义和缩写 Definitions and Acronyms

1.6.1 术语定义一览表 List of Term Definition

术语	定义
GDCA 安全策略委员会	GDCA 认证服务体系内的最高策略管理监督机构和 CP/CPS 一致性决定机构。
电子认证服务机构	负责建立，签发，撤销及管理证书的某个机构。该术语适用于根 CAs 及中级 CAs。
注册机构	注册机构（Registration Authority，RA）负责处理证书申请者和证书订户的服务请求，并将之提交给认证服务机构，为最终证书申请者建立注册过程的实体，负责对证书申请者进行身份标识和鉴别，发起或传递证书撤销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。
证书	使用数字签名的电子文件，用于将公钥与身份绑定。
证书撤销列表	由签发证书的电子认证服务机构（CA）创建并进行数字签名，且定期更新的已撤销证书的带时间戳列表。
电子认证业务规则	构成证书建立，签发，管理及使用管理框架的一份文件。
域名	域名系统中分配至某个节点的标签。
完全限定域名	包括互联网域名系统中所有高级节点标签的域名。
Linting 检测	一种对数字签名数据内容，如预证书（RFC 6962）、证书、证书吊销列表或 OCSP 响应，或待签名数据对象（RFC 5280 第 4.1.1.1 节所述的 tbsCertificate）进行检查的过程，以确保其符合基线要求中定义的配置文件和标准。
在线证书状态协议	在线证书检查协议，可使依赖方应用软件判断某指定证书的状态。
私钥	由密钥对持有者严格保密的密钥对中的密钥，用于创建数字签名，及/或解密通过相应公钥加密的电子记录或文件。
公钥	密钥对中可由相应私钥持有者公开的密钥，可被某个依赖方使用，以核实与持有人相应私钥一并创建的数字签名，及/或可用于加密信息，以便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。
合格的审计师	符合本 CP/CPS 章节 8.2 所述要求的自然人或法律实体。
依赖方	依赖某个有效证书的自然人或法律实体。
订户	被签发证书的自然人或法律实体，且受订户协议或使用条款约束的自然人或法律实体。
订户协议	认证服务机构与证书申请人/订户之间的协议，该协议规定了各方的权力与责任。
WebTrust	CPA 加拿大针对认证服务机构的 WebTrust 项目的现行标准。

Term	Definition
GDCA Security Policy Committee	The highest policy management and supervisory body within the GDCA certification service system, and the authority responsible for determining CP/CPS consistency.
Certification Authority	An organization that is responsible for the creation, issuance, revocation, and management of certificates. The term applies equally to both Roots CAs and Subordinate CAs.
Registration Authority	A Registration Authority (RA) is responsible for processing service requests from certificate applicants and certificate subscribers, and submitting them to the certification authority for the final certificate applicant to establish registration process. RA is also responsible for identifying and verifying certificate applicants, initiating or transferring certificate revocation request, and approving certificate renewal or re-key request on behalf of the certification authority.
Certificate	An electronic document that uses a digital signature to bind a public key and an identity.
Certificate Revocation List	A regularly updated time-stamped list of revoked certificates that is created and digitally signed by the CA that issued the certificates.
Certification Practice Statement	One of several documents forming the governance framework in which certificates are created, issued, managed, and used.
Domain Name	The label assigned to a node in the Domain Name System.
Fully Qualified Domain Name	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
Linting	A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-besigned object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in the TLS BRs.
Online Certificate Status Protocol	An online certificate-checking protocol that enables relying party application software to determine the status of an identified certificate.
Private Key	The key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding public key.
Public Key	The key of a key pair that may be publicly disclosed by the holder of the corresponding private key and that is used by a relying party to verify digital signatures created with the holder's corresponding private key and/or to encrypt messages so that they can be decrypted only

	with the holder's corresponding private key.
Public Key Infrastructure	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of certificates and keys based on public key cryptography.
Qualified Auditor	A natural person or legal entity that meets the requirements of section 8.2 of this CP/CPS.
Relying Party	Any natural person or legal entity that relies on a valid certificate.
Subscriber	A natural person or legal entity to whom a certificate is issued and who is legally bound by a subscriber agreement.
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
WebTrust	The current version of CPA Canada's WebTrust Program for Certification Authorities

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

CA	Certification/Certificate Authority	电子认证服务机构
CAA	Certification Authority Authorization	认证机构授权
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则
CRL	Certificate Revocation List	证书撤消列表
CSR	Certificate Signing Request	证书请求文件
DBA	Doing Business As	商业名称
DNS	Domain Name System	域名系统
EV	Extended Validation	扩展验证/增强验证
FIPS	(US Government) Federal Information Processing Standard	（美国政府）联邦信息处理标准
FQDN	Fully Qualified Domain Name	完全限定域名
GDCA	Global Digital Cybersecurity Authority CO., LTD.	数安时代科技股份有限公司
gTLD	Generic Top-Level Domain	通用顶级域名
IANA	Internet Assigned Numbers Authority	互联网编码分配机构

ICANN	Internet Corporation for Assigned Names and Numbers	互联网名字与编号分配机构
ISO	International Organization for Standardization	国际标准化组织
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
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)
SSL	Secure Sockets Layer	安全套接层
TLS	Transport Layer Security	传输层安全

2. 信息发布与信息管理 Publication and Repository Responsibilities

2.1. GDCA 信息库 Repositories

GDCA 信息库是一个对外公开的信息库，内容包括但不限于以下内容：CP/CPS 现行和历史版本、根证书、中级 CA 证书、CRL、订户协议，以及其它由 GDCA 在必要时发布的信息。GDCA 信息库可以通过网址：https://www.gdca.com.cn 访问，或由 GDCA 随时指定的其它通讯方法获得。

The GDCA repository is a publicly accessible information repository that includes, but is not limited to the current and historical versions of the CP/CPS, root certificates, subordinate CA certificates, CRLs, subscriber agreements, and other information published by GDCA as necessary. The GDCA repository can be accessed at https://www.gdca.com.cn, or through other communication methods designated by GDCA from time to time.

2.2. 信息的发布 Publication of Certification Information

GDCA 在官方网站 https://www.gdca.com.cn 发布信息库，该网站是 GDCA 发布所

有信息首要、最及时、最权威的渠道。订户或依赖方可以通过访问 GDCA 的官网获取根证书、中级 CA 证书的信息和撤销证书列表；同时，GDCA 提供在线证书状态查询服务，订户或依赖方可实时查询证书的状态信息。

GDCA publishes its repository on the official website https://www.gdca.com.cn, which serves as the primary, most timely, and most authoritative channel for all information released by GDCA. Subscribers or relying parties may obtain information regarding root certificates, subordinate CA certificates, and certificate revocation lists by accessing GDCA's official website. In addition, GDCA provides OCSP service, enabling subscribers or relying parties to query certificate status information in real time.

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

对于签发订户证书的 CA，GDCA 应至少每 7 天更新并发布一次 CRL，如有证书被撤销，应在记录该证书撤销状态后 24 小时内更新并发布新的 CRL。

对于签发中级 CA 证书的 CA，GDCA 须至少每 12 个月更新并发布一次 CRL，如有证书被撤销，应在记录该证书撤销状态后 24 小时内更新并发布新的 CRL。

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及有关技术标准的。

For CAs issuing subscriber certificates, GDCA shall update and publish a new CRL at least every seven (7) days. If a certificate is revoked, GDCA shall update and publish a new CRL within twenty-four (24) hours after recording the certificate as revoked.

For CAs issuing subordinate CA certificates, GDCA shall update and publish a new CRL at least every twelve (12) months. If a certificate is revoked, GDCA shall update and publish a new CRL within twenty-four (24) hours after recording the certificate as revoked.

The publication time and frequency of other repository contents are determined independently by GDCA. Such publications shall be timely, efficient, and compliant with national laws and applicable technical standards.

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

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

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

The information in the GDCA repository is publicly available, and anyone may access it. Read-only access to this information is not subject to any restrictions.

GDCA ensures, through cybersecurity protection measures, secure system design, and security

management controls, that only authorized personnel are permitted to add, delete, modify, or publish information in the repository.

3. 身份标识与鉴别 Identification and Authentication

3.1. 命名 Naming

3.1.1. 名称类型 Types of Names

GDCA 颁发的数字证书符合 X.509 标准，分配给证书订户的甄别名采用 X.500 标准命名方式。

The digital certificates issued by GDCA comply with the X.509 standard, and the distinguished names assigned to certificate subscribers adopt the X.500 naming convention.

所有的域名或 IP 地址都添加到主题别名中，而通用名为主域名或 IP 地址，必须是一个出现在主题别名中的域名或 IP 地址。

All domain names or IP addresses are added as the Subject Alternative Name and the common name is a primary domain name which must be one of the domain names or IP addresses from the Subject Alternative Name.

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

GDCA 使用 DN 项来标识证书主体，DN 项中的名称具有一定的代表性意义，应当能够明确确定证书持有机构以及所要标识的网络主机服务器、或互联网域名，并且可以被依赖方识别。

GDCA uses Distinguished Name (DN) attributes to identify the certificate subject. The names contained in the DN have representative significance and shall be sufficient to clearly identify the certificate-holding organization and the network host server or Internet domain name to be identified, and shall be recognizable by relying parties.

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

GDCA 的订户在进行数字证书申请时不能使用匿名或伪名。

Subscribers shall not use anonymous or pseudonymous identities when applying for digital certificates from GDCA.

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

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

The digital certificates issued by GDCA comply with the X.509 Version 3 standard, and the distinguished name format conforms to the X.500 standard. The naming rules for distinguished names are defined by GDCA.

3.1.5. 名称的唯一性 Uniqueness of Names

在 GDCA 信任域内，不同订户的证书的主体甄别名不能相同，必须是唯一的。但对于同一订户，GDCA 可以用其唯一的主体甄别名为其签发多张证书。

Within the GDCA trust domain, the subject distinguished names of certificates issued to different subscribers must be unique and shall not be identical. However, for the same subscriber, GDCA may issue multiple certificates using the same unique subject distinguished name.

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

GDCA 签发的证书的主体甄别名中不包含商标名。

The subject distinguished names of certificates issued by GDCA do not contain trademark names.

3.2. 初始身份确认 Initial Identity Validation

3.2.1. 证明拥有私钥的方法 Method to Prove Possession of Private Key

证书申请者必须证明持有与所要注册公钥相对应的私钥，证明的方法包括在证书申请消息中包含数字签名（PKCS#10）、其它与此相当的密钥标识方法，或者 GDCA 要求的其它证明方式。

The certificate applicant must demonstrate possession of the private key corresponding to the public key to be registered. Acceptable methods of proof include incorporating a digital signature in the certificate request message (PKCS#10), other equivalent key identification methods, or other forms of proof as required by GDCA.

3.2.2. 机构身份和域名的鉴别 Authentication of Organization and Domain Identity

3.2.2.1 机构的身份鉴别 Authentication of Organization Identity

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

方法包括：

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

（2） 通过第三方数据库得到的电话号码、邮政信函、电子邮件等方式与申请机构进行联络，以确认申请者所提供信息的真实性。

（3） 检查组织机构授权给经办人申请办理证书事宜的授权文件及经办人有效身份证件，确保经办人得到申请机构的授权。

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

此外，必要时，GDCA 还可以设定其它所需要的鉴别方式和资料。

申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。

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

Any organization (including government entities, enterprises, or public institutions etc.) applying for an organization-type certificate in the name of the organization shall undergo strict identity authentication. Such authentication may include validating its authenticity through trusted databases and other methods capable of obtaining clear and reliable identity information of the applicant. The certificate application form for an organization subscriber shall bear the signature (or official seal) of the applicant itself or a duly authorized representative of the applicant, indicating acceptance of the relevant terms of the certificate application and assumption of the corresponding responsibilities.

(1) Confirm that the organization is a genuine and legally established entity. Verification methods may include valid documents issued by government authorities, including but not limited to business licenses, organization code certificates of enterprises and public institutions, and verification through authoritative third-party databases maintained by the issuing authorities.

(2) Contact the applicant organization through telephone numbers obtained from third parties, postal correspondence, or other means to verify the authenticity of specific information, such as verifying the position of an agent or confirming whether an individual named in the application form is affiliated with the applicant.

(3) Examine the authorization documents issued by the organization authorizing the handling representative to apply for the certificate, as well as the valid identity documents of the representative, to ensure that the representative has been duly authorized by the applicant organization.

(4) Where deemed necessary, GDCA may also verify the identity of the applicant organization

using information obtained from third parties. If GDCA is unable to obtain all required information from third parties, GDCA may engage third parties to conduct investigations or require the applicant to provide additional information and supporting documentation.

In addition, where necessary, GDCA may establish other required verification methods and documentation requirements.

Applicants are obligated to ensure that the application materials provided are true and valid and shall bear the corresponding legal liabilities.

GDCA establishes evaluation criteria to identify certificate requests that present potential high-risk fraud indicators. Certificate requests identified as “high risk” shall be directly rejected by GDCA.

3.2.2.1.1 EV SSL 订户机构身份的鉴别 Authentication of Organization Identity for EV SSL Subscriber

（1）申请要求

GDCA 仅向机构用户提供 EV SSL 证书申请服务，不为 IP 地址、通配符域名，不为个人签发 EV 证书。机构在申请证书时需按申请证书的类别提交数字证书申请表等相关申请材料，接受证书申请有关的条款，并同意承担相应的责任。

对机构身份的鉴别和审核符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的 EVGs 的要求。同时，当证书申请中包含国际化域名（internationalized domain names，IDNs）时，GDCA 对域名持有人的身份进行验证以检测是否存在 IDNs 的同形异义欺骗（homographic spoofing）行为。

对于申请机构，GDCA 必须进行以下鉴别和验证：

1. 申请者身份及合法存在；
2. 申请者为证书中域名的注册所有者或控制者；
3. 与证书主题中的实体有关的可信的沟通方式；
4. 证书申请经办人必须获得机构授权。

同时，EV 证书申请者必须安排如下角色配合 GDCA 完成审核工作：

1. 经办人：EV 证书申请的提交者以及订单审核的联系人。证书经办人是一个自然人，可以是申请组织的雇员或具有明确授权代表申请组织提交证书申请的授权代理人。
2. 证书审批人：EV 证书请求批准的审批人。证书审批人是一个自然人，可以是申请组织的雇员或具有明确授权代表申请组织批准证书申请的授权代理人。
3. 合同签署人：EV 证书订户协议的签署人。合同签署人是一个自然人，可以是申请组织的雇员或具有明确授权代表申请组织签署订户协议的授权代理人。

申请组织可以授权一个人担任其中的两个或多个角色，申请组织也可以授权一个以上的人担任这些角色中的任何一个。

（2）鉴别要求

- 确认机构身份及合法存在

GDCA 根据 EVGs 第 3.2.2 节中的要求对不同类型的申请机构进行审核，确认机构是确实存在的、合法的实体，包括机构名称、注册编码，及其他注册信息等。GDCA 通过权威第三方数据库进行核查确认。

对于个体工商户、合伙企业等商业实体，GDCA 还需通过视频面对面的方式验证主要负责人。

- 确认申请者的经营地址

GDCA 可以通过以下方式中的一种来进行确认：a）通过权威第三方数据库进行核查确认；b）经验证的可证明申请机构营业地址的专业证明函件。

- 确认申请者运营存在

GDCA 通过以下方式之一进行确认：a）通过登记/注册机构的记录，验证申请机构、附属机构、母公司或子公司至少存在 3 年；b）申请机构、附属机构、母公司或子公司存在于现行的权威第三方数据库中；c）使用已验证的专业证明函件，表明申请机构在受监管的金融机构拥有活跃的活期存款账户。

- 证书申请经办人、合同签署人、证书审批人身份确认

申请机构可以授权一个人来完成多个角色，也可以由多人来完成。GDCA 验证相关人员的身份，并通过已验证的电话、邮件等有效沟通方式与机构进行联系和核实，确认经办人、合同签署人及证书审批人的角色身份（如姓名、职位等）及相关授权。GDCA 以同样方式验证证书申请及订户协议上的签名为真实有效。

- 可信联系方式的确认

GDCA 通过以下方式中的一种来进行确认：a）通过第三方电话公司查询确认；b）通过权威第三方数据库进行确认。可信联系方式可以是电话、传真、邮箱、邮政信函等方式。

(1) Application Requirements

GDCA provides EV SSL certificate application services only to organizational applicants. EV certificates shall not be issued for IP addresses, wildcard domains, or individuals. When applying for a certificate, organizations shall submit a digital certificate application form and other relevant supporting materials according to the certificate type applied for, accept the terms and conditions related to the certificate application, and agree to assume the corresponding responsibilities.

The verification of organizational identity shall comply with the EVGs issued by the CA/Browser Forum at https://cabforum.org.

Where certificate applications contain Internationalized Domain Names (IDNs), GDCA shall verify the identity of the domain name holder to detect and mitigate homographic spoofing risks associated with IDNs.

For applicant organizations, GDCA shall perform the following identification and verification procedures:

1. Verify the identity and legal existence of the Applicant;
2. Verify that the Applicant is the registered owner or controller of the domain name to be included in the certificate;
3. Verify a reliable means of communication associated with the entity identified in the certificate subject;
4. Verify that the Certificate Requester has been duly authorized by the Applicant.

In addition, the following Applicant roles are required for the issuance of an EV Certificate and shall cooperate with GDCA in completing the verification process:

1. Certificate Requester: The individual who submits the EV Certificate Request and serves as the contact person for certificate request verification. The Certificate Requester shall be a natural person who may either be an employee of the Applicant or an authorized agent expressly authorized to submit EV Certificate Requests on behalf of the Applicant.
2. Certificate Approver: The individual responsible for approving the EV Certificate Request. The Certificate Approver shall be a natural person who may either be an employee of the Applicant or an authorized agent expressly authorized to approve EV Certificate Requests on behalf of the Applicant.
3. Contract Signer: The individual who signs the EV Certificate Subscriber Agreement. The Contract Signer shall be a natural person who may either be an employee of the Applicant or an authorized agent expressly authorized to sign the Subscriber Agreement on behalf of the Applicant.

The Applicant may authorize one individual to occupy two or more of these roles. The Applicant may also authorize more than one individual to occupy any of these roles.

(2) Authentication Requirements

- Verification of organizational identity and legal existence

GDCA shall conduct verification of different types of applicants in accordance with Section 3.2.2 of the EVGs. GDCA shall confirm that the applicant is a valid and legally existing entity, including its legal name, registration number, and other registration information. Verification shall be performed through authoritative third-party databases.

For sole proprietorships, partnerships, and other similar business entities, GDCA shall additionally verify the identity of the principal representative through video-based face-to-face verification.

- Verification of Applicant’s physical address

GDCA shall verify the Applicant's physical address using one of the following methods:

a) verification through authoritative third-party databases; or

b) a verified professional reference letter capable of evidencing the Applicant's business address.

- Verification of Applicant operational existence

GDCA shall verify the Applicant's operational existence using one of the following methods: a) verification through records of the registration authority confirming that the Applicant, affiliated entity, parent company, or subsidiary has existed for at least three (3) years; b) confirmation that the Applicant, affiliated entity, parent company, or subsidiary appears in a current authoritative third-party database; or c) a verified professional reference letter demonstrating that the Applicant maintains an active demand deposit account with a regulated financial institution.

- Verification of identity of Certificate Requester, Contract Signer, and Certificate Approver

The Applicant may authorize one individual to fulfill multiple roles, or multiple individuals may be assigned to these roles. GDCA shall verify the identity of the relevant individuals and confirm, through validated communication methods such as telephone and email, the roles and authorization of the Certificate Requester, Contract Signer, and Certificate Approver (including name, title, etc.). GDCA shall also verify the authenticity of signatures on the certificate application and the Subscriber Agreement using the same methods.

- Verification of reliable means of communication

GDCA shall verify a reliable means of communication using one of the following methods: a) confirmation via a third-party telephone service provider; or b) verification through authoritative third-party databases. Reliable means of communication may include telephone, facsimile, email, or postal mail.

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

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

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

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

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the applicant's legal creation, existence, or recognition;
2. A reliable data source;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An attestation letter accompanied by documentary support; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that GDCA determines to be reliable.

3.2.2.3 所在国的确认与鉴别 Verification of Country

若证书主题项中包含国家选项，GDCA 通过权威第三方数据库查询网站 DNS 记录显示的 IP 地址或申请者的 IP 地址来确认所在国，确保申请人的 IP 地址所在国与申请人实际所在国一致。

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

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

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

1. 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。随机值的验证方法为：（1）GDCA 向该邮件地址发送随机值，随机值由系统产生，并且唯一；（2）申请者收到邮件并回复该随机值进行确认；（3） GDCA 收到回复，并将回复中的随机值与发送的随机值进行比对，若比对结果一致，则鉴别通过。随机值的有效期最大为产生该随机值开始的 30 天。鉴别方式遵循 TLS BRs 第 3.2.2.4.4 节。
2. 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 TLS BRs 第 3.2.2.4.7 节。GDCA 按照本 CP/CPS 第 3.2.2.9 节的规定实施多视角签发验证（MPIC）。为了计入验证结果，网络视角必须监测到与主网络视角相同的挑战信息（即随机值或请求令牌）。

3. 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 TLS BRs 第 3.2.2.4.18 节。GDCA 按照本 CP/CPS 第 3.2.2.9 节的规定实施多视角签发验证（MPIC）。为了计入验证结果，网络视角必须监测到与主网络视角相同的挑战信息（即随机值或请求令牌）。

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

1. Sending an constructed email to domain contact to confirm the ownership and control of the domain name, by sending an email including a Random Value to one or more addresses created by using 'admin', 'administrator', 'webmaster','hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an authorized Domain Name, and receiving a confirming response utilizing the Random Value. The validation steps include: (1) GDCA sends a Random Value to such e-mail address and the Random Value will be generated by a system to ensure its uniqueness; (2) The applicant receives the Random Value via an e-mail and sends back a confirming response with such Random Value; (3) GDCA receives the Random Value from the applicant and compare such value with the one sent by GDCA, the validation completes once GDCA confirms that the Random Value received matches the one it sends. The Random Value remains valid for use in a confirming response for no more than 30 days from its creation. This way of validation conforms to section 3.2.2.4.4 of the TLS BRs.

2. By confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record to confirm the applicant’s practical control over the FQDN. This way of validation conforms to section 3.2.2.4.7 of the TLS BRs. GDCA implements Multi-Perspective Issuance Corroboration as specified in section 3.2.2.9 of this CP/CPS. To count as corroborating, a network perspective must observe the same challenge information (i.e. Random Value or Request Token) as the primary network perspective.

3. Confirming the applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file (such as a Request Token, Random Number that does not appear in the request used to retrieve the file and receipt of a successful HTTP 2xx status code response from the request). This way of validation conforms to section 3.2.2.4.18 of the TLS BRs. GDCA implements Multi-Perspective Issuance Corroboration as specified in section 3.2.2.9 of this CP/CPS. To count as corroborating, a network perspective must observe the same challenge information (i.e. Random Value or Request Token) as the primary network perspective.

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

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

视角下所有域名授权或控制权验证相关 DNS 查询的 DNS 解析器必须：

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

自 2026 年 3 月 15 日起：

对于本节第 1 种域名鉴别方式中描述的构建电子邮件的验证方法，通过主网络视角执行的与域名授权或控制权验证相关的所有基于 DNS CNAME、CAA、TXT 的查询以尝试获取授权域名，GDCA 必须执行基于 IANA DNSSEC 根信任锚的 DNSSEC 验证，且不得使用本地策略禁用 DNSSEC 验证。对于所有其他的 DNS 查询，应执行基于 IANA DNSSEC 根信任锚的 DNSSEC 验证，并且 GDCA 不应该使用本地策略来禁用 DNSSEC 验证。

对于所有其他的域名验证方法，从主网络视角执行的所有与域名授权或控制权验证相关的 DNS 查询，GDCA 必须执基于 IANA DNSSEC 根信任锚的 DNSSEC 验证。GDCA 不得使用本地策略禁用任何与域名授权或控制权验证相关的 DNS 查询的 DNSSEC 验证。

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

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

基于 IANA DNSSEC 根信任锚的 DNSSEC 验证不在本 CP/CPS 第 5.4.1 节中的日志记录范围内。

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

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

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

Effective March 15, 2026:

For e-mail Domain Validation methods described in section 3.2.2.4.1, DNSSEC validation back to the IANA DNSSEC root trust anchor must be performed on all DNS CNAME, CAA, TXT queries attempting to obtain the authorization domain name associated with the validation of domain authorization or control by the Primary Network Perspective and GDCA must not use local policy to disable DNSSEC validation. For all other DNS queries, DNSSEC validation back to the IANA DNSSEC root trust anchor should be performed and GDCA should not use local policy to disable DNSSEC validation.

For all other Domain Validation methods, DNSSEC validation back to the IANA DNSSEC root trust anchor must be performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective and GDCA must not use local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control.

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

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

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of the logging requirements of section 5.4.1 of this CP/CPS.

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

GDCA 采用以下方式，确认申请者拥有或实际控制该 IP 地址：

1. 在包含 IP 地址的 URI(统一资源标识符)的在线网页上对约定的信息进行改动，通过此方式以确认申请者对 IP 地址的实际控制权。鉴别方式遵循 TLS BRs 第 3.2.2.5.1 节。GDCA 按照本 CP/CPS 第 3.2.2.9 节的规定实施多视角签发验证（MPIC）。为了计入验证结果，网络视角必须监测到与主网络视角相同的挑战信息（即随机值或请求令牌）。

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

1. By making a change to the agreed-upon information found on an online Web page identified by a uniform resource identifier containing the IP address, to confirm the applicant's practical control over the IP address. This way of validation conforms to section 3.2.2.5.1 of the TLS BRs. GDCA implements Multi-Perspective Issuance Corroboration as specified in section 3.2.2.9 of this CP/CPS. To count as corroborating, a network perspective must observe the same challenge information (i.e. Random Value or Request Token) as the primary network perspective.

3.2.2.6 通配符域名确认 Wildcard Domain Validation

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

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

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

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

3.2.2.7 数据来源的准确性 Data Source Accuracy

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

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

若从评估为可依赖数据来源中获得的数据或文件的时间不超过证书签发前 398 天，则 GDCA 可使用该数据及文件。对于根据本 CP/CPS 3.2.2.4 对域名和本 CP/CPS 3.2.2.5 对 IP 地址进行的验证，所使用的任何数据、文件或已完成的验证，必须在签发证书之前且在下表所规定的最长期限（以天为单位）内获取或完成。

证书颁发日期当天或之后	证书颁发日期在当天之前	最大重用时长
	2026 年 3 月 15 日	398 天
2026 年 3 月 15 日	2027 年 3 月 15 日	200 天
2027 年 3 月 15 日	2029 年 3 月 15 日	100 天
2029 年 3 月 15 日		10 天

2020 年 10 月 1 日起，在使用某个实体登记/注册机构以满足 EV SSL 证书有关审核验证要求之前，GDCA 确保必须通过本 CP/CPS 章节 2.1 中所述的 GDCA 信息库，公开

披露 EV SSL 证书审核验证所使用的实体登记/注册机构数据来源。其他类型的证书遵循该数据来源来进行机构身份的审核验证。

实体登记/注册机构的信息必须至少涵盖以下内容：

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

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

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

GDCA may use the documents and data to verify certificate information, provided that it obtained the data or document no more than 398 days prior to issuing the certificate. For validation of domain names and IP addresses according to Section 3.2.2.4 and Section 3.2.2.5 of this CP/CPS, any data, document, or completed validation used must be obtained within the maximum number of days prior to issuing the certificate, as defined in the following table:

Certificate issued on or after	Certificate issued before	Maximum data reuse period
	March 15, 2026	398 days
March 15, 2026	March 15, 2027	200 days
March 15, 2027	March 15, 2029	100 days
March 15, 2029		10 days

Effective as of 1 October 2020, GDCA shall ensure that, prior to the use of an Incorporating Agency or Registration Agency to fulfill the verification requirements for EV SSL certificates; the Incorporating Agency or Registration Agency data sources used for EV SSL Certificates will be

publicly disclosed in the repository described in section 2.1 of this CP/CPS. GDCA also uses this data sources to validate the identities of organizations for other types of certificates.

This Agency Information shall include at least the following:

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

3.2.2.8 认证机构授权记录 CAA Records

GDCA 对签发证书主题别名扩展项中的每一个 dNSName 做 CAA 记录检查，并遵循查询到的指示。

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

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

GDCA checks the CAA records and follow the processing instructions found for each dNSName in the subjectAltName extension of the certificate to be issued.

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

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

3.2.2.9 多视角签发验证 Multi-Perspective Issuance Corroboration

多视角签发验证旨在在证书签发之前，通过来自多个远程网络视角的验证结果，对

主网络视角所做出的判定（例如，域名验证通过/失败、CAA 许可/禁止）进行佐证。该过程有助于增强对等前缀的边界网关协议（BGP）攻击或劫持的防护能力。

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

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

a. 存在符合预期的：1)随机值，2)请求令牌，3) IP 地址，或 4)联系地址。上述内容均应符合本 CP/CPS 第 3.2.2.4 和 3.2.2.5 节中规定的验证方法要求；以及

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

本 CP/CPS 第 3.2.2.4 节和第 3.2.2.5 节描述了需要使用多视角签发验证的方法，以及网络视角如何对主网络视角所确定的结果进行佐证。

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

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

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

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

网络视角与主网络视角及组成一致性数量的其他网络视角不同地点时，该网络视角被视为远程的。

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

多视角验证一致性要求表

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

执行多视角签发验证的远程网络视角应符合以下要求：

必须执行：

- 网络加固

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

应当执行：

- 设施与服务提供商要求
  - 部署于通过 ISO/IEC 27001 认证或具备同等安全框架、并已独立审计和认证或报告的设施。
  - 所依赖的服务应包含以下报告之一：系统与组织控制报告 2（SOC 2）、IASE 3000、ENISA 715、FedRAMP Moderate、C5:2020、CSA STAR CCM，或其他经独立审计、认证或报告的等效服务框架。
- 漏洞检测与补丁管理
  - 实施入侵检测与防御控制措施，以防御常见的网络和系统威胁。
  - 建立并执行漏洞修复流程，包括漏洞的识别、审查、响应与修复。
  - 至少每三（3）个月进行一次漏洞扫描。
  - 至少每年进行一次渗透测试。
  - 在安全补丁发布后六（6）个月内应用推荐的安全补丁，除非 GDCA 记录证明该补丁会引入新的漏洞或系统不稳定，从而导致风险超过修补收益。
- 系统加固
  - 禁用所有未使用的账户、应用程序、服务、协议和端口。
  - 为所有用户账户实施多因素认证。

- 网络加固
  - 配置每个网络边界控制设备（防火墙、交换机、路由器、网关或其他网络控制系统），仅允许其运行所需的服务、协议、端口和通信。
  - 依赖的网络（如互联网服务提供商）应当：1）使用基于安全域间路由（RFC 6480）的机制，例如 BGP 前缀来源验证（RFC 6811）；2）使用其他非 RPKI 的路由泄露防护机制（如 RFC 9234）；3）遵循 BCP 194 中描述的当前最佳实践。建议在正常运行条件下，执行多视角签发验证的网络视角应通过过滤 RFC 6811 定义的 RPKI 无效 BGP 路由的网络或网络集合转发所有互联网流量，但这并非强制要求。

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

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

分阶段实施时间表：

自 2024 年 9 月 15 日起：

GDCA 应当使用至少两个（2）远程网络视角实施多视角签发验证。

自 2025 年 3 月 15 日起：

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

自 2025 年 9 月 15 日起：

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

自 2026 年 3 月 15 日起：

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

自 2026 年 6 月 15 日起：

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

自 2026 年 12 月 15 日起：

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

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

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

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

a. the presence of the expected 1) Random Value, 2) Request Token, 3) IP Address, or 4) Contact Address, as required by the relied upon validation method specified in sections 3.2.2.4 and 3.2.2.5 of this CP/CPS; and

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

Sections 3.2.2.4 and 3.2.2.5 of this CP/CPS describe the validation methods that require the use of Multi-Perspective Issuance Corroboration and how a network perspective can corroborate the outcomes determined by the primary network perspective.

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

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

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

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

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

Quorum Requirements Table

Distinct Remote Network Perspectives Used	Allowed non-Corroborations
2-5	1
6+	2

Remote network perspectives performing Multi-Perspective Issuance Corroboration:

MUST:

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

SHOULD:

- Facility & Service Provider Requirements
  - Be hosted from an ISO/IEC 27001 certified facility or equivalent security framework independently audited and certified or reported.
  - Rely on services covered in one of the following reports: System and Organization Controls 2 (SOC 2), IASE 3000, ENISA 715, FedRAMP Moderate, C5:2020, CSA STAR CCM, or equivalent services framework independently audited and certified or reported.
- Vulnerability Detection and Patch Management

- Implement intrusion detection and prevention controls to protect against common network and system threats.
- Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities.
- Undergo or perform a Vulnerability Scan at least every three (3) months.
- Undergo a Penetration Test on at least an annual basis.
- Apply recommended security patches within six (6) months of the security patch's availability, unless GDCA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

- System Hardening
  - Disable all accounts, applications, services, protocols, and ports that are not used.
  - Implement multi-factor authentication for all user accounts.
- Network Hardening
  - Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications identified as necessary to its operations.
  - Rely upon networks (e.g., Internet Service Providers) that: 1) use mechanisms based on Secure Inter-Domain Routing (RFC 6480), for example, BGP Prefix Origin Validation (RFC 6811), 2) make use of other non-RPKI route-leak prevention mechanisms (such as RFC 9234), and 3) apply current best practices described in BCP 194. While it is recommended that under normal operating conditions Network Perspectives performing Multi-Perspective Issuance Corroboration forward all Internet traffic via a network or set of networks that filter RPKI-invalid BGP routes as defined by RFC 6811, it is not required.

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

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

Phased Implementation Timeline:

- **Effective September 15, 2024**, GDCA should implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives.
- **Effective March 15, 2025**, GDCA shall implement Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. GDCA may proceed with certificate issuance if the number of remote Network Perspectives that do not corroborate the determinations made by the Primary Network Perspective ("non-corroborations") is greater than allowed in the Quorum Requirements table.

- **Effective September 15, 2025**, GDCA shall implement Multi- Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. GDCA shall ensure that the requirements defined in Quorum Requirements Table are satisfied. If the requirements are not satisfied, GDCA shall not proceed with issuance of the certificate.
- **Effective March 15, 2026,** GDCA shall implement Multi-Perspective Issuance Corroboration using at least three (3) remote Network Perspectives. GDCA shall ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then GDCA shall not proceed with issuance of the certificate.
- **Effective June 15, 2026**, GDCA shall implement Multi-Perspective Issuance Corroboration using at least four (4) remote Network Perspectives. GDCA shall ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then GDCA shall not proceed with issuance of the certificate.
- **Effective December 15, 2026**, GDCA shall implement Multi-Perspective Issuance Corroboration using at least five (5) remote Network Perspectives. GDCA shall ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then GDCA shall not proceed with issuance of the certificate.

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

GDCA 不向自然人签发 SSL/TLS 证书。

GDCA does not issue SSL/TLS certificates to natural persons.

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

证书中的信息必须经过验证，未经验证的信息不得写入证书。

All information included in a certificate shall be verified. Information that has not been verified shall not be included in the certificate.

3.2.5. 授权确认 Validation of Authority

当机构订户授权经办人办理证书业务时，GDCA 进行如下验证：

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

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

Where an organizational subscriber authorizes a representative to handle certificate-related matters, GDCA shall perform the following verification procedures:

1. Verify the existence of the organization through methods such as third-party identity verification services or databases, or documents issued by competent government authorities;
2. Verify, through telephone calls, postal correspondence with proof of delivery, employment verification, or equivalent methods that the individual belongs to the organization and is duly authorized by the organization to act on its behalf.

GDCA permits an applicant to designate specific individuals to submit certificate requests. Where the Applicant has designated, in writing, specific individuals authorized to request certificates, GDCA shall not accept certificate requests from any individual other than those designated persons.

Upon receipt of a verified written request from the applicant, GDCA shall provide the applicant with a list of its authorized individuals.

3.2.6. 互操作准则 Criteria for Interoperation

对于其他的电子认证服务机构，可以与 GDCA 进行互操作，但是该电子认证服务机构的 CPS 必须符合 GDCA CP/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。

Other electronic certification service providers may interoperate with GDCA; however, the CPS of such certification service providers shall comply with the requirements of GDCA's CP/CPS, and appropriate agreements shall be executed with GDCA.

GDCA may, in accordance with the terms of such agreements, accept identity verification information validated by non-GDCA issuing authorities and issue corresponding certificates based on such information.

To date, GDCA has not issued any cross-certificates.

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

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

Prior to the expiration of a subscriber certificate, the subscriber shall obtain a new certificate in order to maintain continuity of certificate usage. GDCA generally requires the subscriber to generate a new key pair to replace the expiring key pair, which is referred to as “Re-key”

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

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

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

For routine re-key requests under normal circumstances, the subscriber shall submit sufficient information capable of identifying the original certificate, such as the subscriber Distinguished Name and certificate serial number. Authentication of the request shall be based on the following aspects:

- Confirmation that the original certificate corresponding to the request exists and was issued by GDCA;
- Verification of the signature on the request using the subscriber public key contained in the original certificate;
- Identity verification based on the original registration information.

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

GDCA 不提供证书被撤销后的密钥更新。

GDCA does not provide re-key services after a certificate has been revoked.

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

当 GDCA 有本 CP/CPS 4.9.1.1 所述理由需要撤销订户的证书时，有权撤销证书，这种情况无须进行鉴别。如果订户主动要求撤销证书，则按照本 CP/CPS 第 3.2 节描述进行身份鉴别。

Where GDCA has grounds to revoke a subscriber certificate as described in Section 4.9.1.1 of this CP/CPS, it shall have the authority to revoke the certificate without further authentication.

Where the Subscriber voluntarily requests certificate revocation, identity verification shall be performed in accordance with section 3.2 of this CP/CPS.

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

GDCA 自行担任证书 RA，不再另行设立 RA。

GDCA serves as RA by itself and does not assign another RA.

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

4.1. 证书申请 Certificate Application

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

证书申请实体包括个人和具有独立法人资格的组织机构(包括国家机关、事业单位、社会团体等)。

The certificate applicant entities include individuals and organizations with independent legal personality (including government agencies, public institutions, social organizations etc.).

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

证书注册操作符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的要求。注册流程包括使用安全的方法生成密钥对，提交包含所有必要信息（包括公钥）的证书申请请求。申请者应事先了解订户协议、本 CP/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。

订户有责任向 GDCA 提供真实、完整和准确的证书申请信息和资料。

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，同时承担相应审核责任。

The certificate enrollment process complies with the requirements published by the CA/Browser Forum at www.cabforum.org. The enrollment process includes the use of secure methods to generate key pairs and the submission of certificate signing requests containing all necessary information, including the public key. Applicants shall review in advance the provisions set forth in documents such as the Subscriber Agreement and this CP/CPS, particularly those related to the scope of certificate usage, rights, obligations, and warranties.

Subscribers are responsible for providing GDCA with truthful, complete, and accurate information

and documentation for certificate applications.

GDCA is responsible for verifying the consistency between the certificate application information provided by subscribers and their identity verification documents, and assumes corresponding review responsibilities.

4.2. 证书申请处理 Certificate Application Processing

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

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

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

若从评估为可依赖数据来源中获得的数据或文件的时间不超过证书签发前 398 天，则 GDCA 可使用该数据及文件。对于根据本 CP/CPS 3.2.2.4 对域名和本 CP/CPS 3.2.2.5 对 IP 地址进行的验证，所使用的任何数据、文件或已完成的验证，必须在签发证书之前且在下表所规定的最长期限（以天为单位）内获取或完成。

证书颁发日期当天或之后	证书颁发日期在当天之前	最大重用时长
	2026 年 3 月 15 日	398 天
2026 年 3 月 15 日	2027 年 3 月 15 日	200 天
2027 年 3 月 15 日	2029 年 3 月 15 日	100 天
2029 年 3 月 15 日		10 天

Upon receiving a certificate application from a subscriber, GDCA shall perform identity identification and authentication of the subscriber in accordance with Section 3.2 of this CP/CPS.

During the certificate application processing, GDCA shall ensure, through effective means, that the certificate information corresponds to the correct application information and shall issue the certificate to the correct applicant.

GDCA may use the documents and data to verify certificate information, provided that it obtained the data or document no more than 398 days prior to issuing the certificate. For validation of domain names and IP addresses according to Section 3.2.2.4 and Section 3.2.2.5 of this CP/CPS, any data, document, or completed validation used must be obtained within the maximum number of days prior to issuing the certificate, as defined in the following table:

Certificate issued on or after	Certificate issued before	Maximum data reuse period
	March 15, 2026	398 days
March 15, 2026	March 15, 2027	200 days

March 15, 2027	March 15, 2029	100 days
March 15, 2029		10 days

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

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

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

After GDCA has successfully completed all required verification steps for the certificate application and submitted the certificate request, the certificate application is approved through the issuance of a certificate by GDCA.

GDCA may approve a certificate application if the following conditions are met:

1. The application fully complies with the subscriber identification and authentication requirements specified in Section 3.2 of this CP/CPS;
2. The applicant has accepted, or has not objected to, the terms and requirements of the Subscriber Agreement;
3. The applicant has duly paid the applicable fees as required.

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

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 3.2 关于订户身份的标识和鉴别规定；
2) 申请者不能提供所需要的身份证明材料；
3) 申请者反对或者不能接受订户协议的有关内容和要求；
4) 申请者没有或者不能够按照规定支付相应的费用；
5) 申请的证书含有 ICANN（The Internet Corporation for Assigned Names and Numbers）考虑中的新 gTLD（顶级域名）；
6) GDCA 认为批准该申请将会对 GDCA 带来争议、法律纠纷或者损失。

GDCA shall reject a certificate application if any of the following conditions occur:

1. The application does not comply with the subscriber identification and authentication requirements

specified in Section 3.2 of this CP/CPS;

2. The applicant is unable to provide the required identity verification documents;
3. The applicant objects to or cannot accept the relevant terms and requirements of the Subscriber Agreement;
4. The applicant has not paid, or is unable to pay, the applicable fees as required;
5. The requested certificate contains a new gTLD (generic top-level domain) under consideration by ICANN (the Internet Corporation for Assigned Names and Numbers);
6. GDCA determines that approving the application may result in disputes, legal liability, or losses to GDCA.

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

对于拒绝的证书申请，GDCA 通知申请者证书申请失败。

GDCA shall reject an application if it is explicitly prohibited by laws or regulations, or if GDCA determines that approving the application presents a high risk. GDCA establishes and maintains a list of high-risk certificate applicants based on information from third parties such as anti-phishing alliances, antivirus vendors, relevant industry alliances, and government authorities responsible for cybersecurity, as well as information disclosed in public media reports, or records of certificate requests previously rejected or certificates revoked by GDCA due to suspected phishing or other fraudulent activities or concerns. GDCA will check this list when processing certificate applications, and applications submitted by applicants appearing on the list shall be directly rejected.

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

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

GDCA 将做出合理努力来尽快确认证书申请信息，将在 2 个工作日内处理证书申请。

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

GDCA will make reasonable efforts to verify certificate application information as promptly as possible and will process certificate applications within two (2) business days.

Whether GDCA can process a certificate application within the above time frame depends on whether the applicant has submitted true, complete, and accurate information and has responded in a timely manner to GDCA's requirements.

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

GDCA 对签发证书主题别名扩展项中的每一个 dNSName 做 CAA 记录检查，并遵循查询到的指示。

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

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

GDCA checks the CAA records and follow the processing instructions found for each dNSName in the subjectAltName extension of the certificate to be issued.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.3. 证书签发 Certificate Issuance

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

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

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

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

GDCA 在批准证书申请之后，将签发证书。证书的签发意味着 GDCA 最终完全正式地批准了证书申请。

对于 2025 年 3 月 15 日当天或之后签发的 SSL/TLS 证书，在证书签发之前，GDCA

必须对待签名证书（TBS 证书）进行 linting 检测。

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

During the certificate issuance process, the RA administrator is responsible for approving certificate applications and, through operation of the RA system, submitting certificate issuance requests to the CA's certificate issuance system. The certificate issuance request information sent from the RA to the CA shall be subject to RA authentication and information protection measures, and shall ensure that the request is delivered to the correct CA certificate issuance system.

Upon receiving a certificate issuance request from the RA, the CA's certificate issuance system shall authenticate and decrypt the information from the RA. For valid certificate issuance requests, the system shall issue subscriber certificates.

After approving the certificate application, GDCA will issue the certificate. The issuance of a certificate signifies that GDCA has formally and fully approved the certificate application.

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

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

GDCA 的证书签发系统签发证书后，将通知订户证书已被签发，并告知订户如何获得证书。

After the GDCA certificate issuance system issues a certificate, GDCA will notify the subscriber that the certificate has been issued and inform the subscriber how to obtain the certificate.

4.4. 证书接受 Certificate Acceptance

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

订户被认为接受已签发的证书的行为包括但不仅限于：

1. 订户自行访问专门的 GDCA 证书服务网站将证书下载，证书下载完毕即代表订户接受了证书。
2. GDCA 在订户的允许下，代替订户下载证书，并把证书通过邮件及其他 GDCA 认为可靠方式发送给订户，即代表订户接受了证书。
3. 订户接受了获得证书的方式，并且没有提出反对证书或者证书中的内容。

A subscriber is deemed to have accepted an issued certificate through conducts including, but not limited to, the following:

1. The subscriber independently accesses the designated GDCA certificate service website to download the certificate, the completion of the download constitutes acceptance of the certificate.
2. With the subscriber's authorization, GDCA downloads the certificate on behalf of the subscriber and delivers it to the subscriber via email or other reliable methods deemed appropriate by GDCA; such delivery constitutes acceptance of the certificate by the subscriber.
3. The subscriber accepts the method of obtaining the certificate and raises no objection to the certificate or its contents.

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

订户接受证书后，GDCA 在 24 小时内将该订户证书发布到 GDCA 的目录服务系统。同时，GDCA 根据 Google 的 CT 策略（https://github.com/chromium/ct-policy），将订户的域名信息发布在至少三个 CT 服务器中。

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

After a subscriber accepts the certificate, GDCA will publish the subscriber's certificate to its directory service system within 24 hours. In addition, in accordance with Google's Certificate Transparency (CT) policy (https://github.com/chromium/ct-policy), GDCA will publish the subscriber's domain information to at least three CT logs.

GDCA adopts a master–secondary directory server architecture for distributing issued certificates. Upon issuance, certificate data is first published to the primary directory server and then automatically synchronized to secondary directory servers through master-secondary mapping, enabling access and download by subscribers and relying parties.

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

对于已签发的证书，GDCA 将不对其他实体进行通告。

For issued certificates, GDCA will not notify any other entities.

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

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

订户在接受了 GDCA 所签发的证书后，均视为已经同意遵守与 GDCA、依赖方有关的权利和义务的条款。订户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。

After accepting a certificate issued by GDCA, the subscriber is deemed to have agreed to comply with the terms and conditions governing the rights and obligations between GDCA and relying parties. The subscriber shall take reasonable measures to properly safeguard the corresponding private key and prevent unauthorized use.

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

依赖方应：

1. 在依赖证书前核验证书状态，包括查询证书撤销信息；
2. 确保证书仅用于其预定用途，并且在证书有效期内使用；
3. 仅在本 CP/CPS 及相关协议规定的范围内依赖证书。

是否依赖某一证书的决定及其后果，由依赖方自行负责。

Relying parties shall:

1. Verify the status of a certificate prior to reliance, including checking revocation information
2. Ensure that the certificate is used only for its intended purpose and within its validity period
3. Rely on a certificate only to the extent permitted by this CP/CPS and applicable agreements

The decision to rely on a certificate shall remain the sole responsibility of the relying party.

4.6. 证书更新 Certificate Renewal

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

订户需按新申请的要求提交注册信息。

Subscribers shall submit registration information in accordance with the requirements for a new application.

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

请求证书更新的实体为证书订户。

The entity who requests certificate update is the subscriber.

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

订户可选择一般的初始证书申请流程进行证书更新，按照本 CP/CPS 第 3.2 节的要求提交相应的证书申请和身份证明资料。GDCA 将这种初始证书申请的鉴别方式作为证书更新时的鉴别处理手段。

Subscribers may choose to use the initial certificate application process for certificate renewal and shall submit the corresponding certificate application and identity verification materials in

accordance with Section 3.2 of this CP/CPS. GDCA will treat the identity verification method used in the initial certificate application process as the authentication procedure for certificate renewal.

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

同本 CP/CPS 第 4.3.2 节。

See CP/CPS Section 4.3.2.

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

同本 CP/CPS 第 4.4.1 节。

See CP/CPS Section 4.4.1.

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

同本 CP/CPS 第 4.4.2 节。

See CP/CPS Section 4.4.2.

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

同本 CP/CPS 第 4.4.3 节。

See CP/CPS Section4.4.3.

4.7. 证书密钥更新 Certificate Rekey

证书密钥更新指订户生成一对新密钥并申请为新公钥签发一个新证书。

Certificate Rekey refers to the process in which a subscriber generates a new key pair and applies for the issuance of a new certificate corresponding to the new public key.

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

订户可在需要时申请密钥更新。

Subscribers may apply for rekey update when necessary.

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

请求证书密钥更新的实体为证书订户。

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

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

同本 CP/CPS 第 3.3 节。

See section 3.3 of this CP/CPS.

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

同本 CP/CPS 第 4.3.2 节。

See CP/CPS Section 4.3.2.

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

同本 CP/CPS 第 4.4.1 节。

See CP/CPS Section 4.4.1.

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

同本 CP/CPS 第 4.4.2 节。

See CP/CPS Section 4.4.2.

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

同本 CP/CPS 第 4.4.3 节。

See CP/CPS Section 4.4.3.

4.8. 证书变更 Certificate Modification

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

如果订户提供的注册信息发生改变，必须向 GDCA 提出证书变更。证书变更的申请和证书申请所需的流程、条件是一致的。

If any of the registration information provided by the subscriber changes, the subscriber must submit a certificate change request to GDCA. The procedures and requirements for certificate change requests are the same as those for certificate applications.

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

请求证书变更的实体为证书订户。

The entity requesting certificate modification is the certificate subscriber.

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

证书变更按照初次申请证书的注册过程进行处理。

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

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

同本 CP/CPS 第 4.3.2 节。

See CP/CPS Section 4.3.2.

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

同本 CP/CPS 第 4.4.1 节。

See CP/CPS Section 4.4.1

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

同本 CP/CPS 第 4.4.2 节。

See CP/CPS Section 4.4.2.

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

同本 CP/CPS 第 4.4.3 节。

See CP/CPS Section 4.4.3.

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

4.9.1. 证书撤销的情形 Circumstances for Revocation

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

若出现以下情况中的一种或多种，GDCA 必须在 24 小时之内撤销证书：

1. 订户以书面形式请求撤销证书；
2. 订户通知 GDCA 最初的证书请求未得到授权且不能追溯到授权行为；
3. GDCA 获得了证据，证明与证书公钥对应订户私钥遭到了泄漏；
4. GDCA 获得了证据，证明对证书中 FQDN，IP 地址或邮箱地址的域名授权或控制权的验证不应被依赖，包括 GDCA 未能正确执行 CAA 检查或根据本 CP/CPS 第 4.2.4 节不允许签发的情况；
5. CA 被告知出现了可使订户私钥泄露的经验证的方法，此类方法可根据公钥轻易地计算私钥值（例如 Debian 弱密钥，见：http://wiki.debian.org/SSLkeys），或存在明确的证据。

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

1. 证书不再符合 TLS BRs 第 6.1.5 节及第 6.1.6 节的相关要求；
2. GDCA 获得了证书遭到误用的证据；
3. GDCA 获悉订户违反了订户协议、CP/CPS 中的一项或多项重大责任；
4. GDCA 获悉了任何表明 FQDN 或 IP 地址的使用不再被法律许可（例如，某法院或仲裁员已经撤销了域名注册人使用域名的权力）；
5. GDCA 获悉某通配符证书被用于鉴别具有欺骗误导性的子域名；
6. GDCA 获悉证书中所含信息出现重大变化；
7. GDCA 获悉证书的签发未能符合 TLS BRs 要求或 GDCA 的 CP/CPS；
8. GDCA 认为任何或被告知出现在证书中的信息为错误信息；
9. GDCA 依据 TLS BRs 签发证书的权力失效，或被撤销或被终止，除非其继续维

护 CRL/OCSP 信息库；

10. CP/CPS 中职责的履行被延迟或受不可抗力的阻碍；自然灾害；计算机或通信失败；法律、规章或其它法律的改变；政府行为；或其它超过个人控制的原因并且对他人信息构成威胁的；
11. GDCA 已经履行催缴义务后，订户仍未缴纳服务费。

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

1. The subscriber requests in writing that GDCA revoke the certificate;
2. The subscriber notifies GDCA that the original certificate request was not authorized and does not retroactively grant authorization;
3. GDCA obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise; or
4. GDCA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name. IP address or mailbox address in the certificate should not be relied upon, including cases where GDCA failed to perform CAA checking correctly or where issuance was not permitted according to section 4.2.4 of this CP/CPS; or
5. GDCA is made aware of a demonstrated or proven method that exposes the subscriber's private key to compromise, methods have been developed that can easily calculate it based on the public key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).

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

1. The certificate no longer complies with the TLS BRs section 6.1.5 and 6.1.6;
2. GDCA obtains evidence that the certificate was misused;
3. GDCA is made aware that a subscriber has violated one or more of its material obligations under the subscriber agreement and CP/CPS;
4. GDCA is made aware of any circumstance indicating that use of a fully-qualified domain name or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a domain name registrant's right to use the domain name);
5. GDCA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name;
6. GDCA is made aware of a material change in the information contained in the certificate;
7. GDCA is made aware that the certificate was not issued in accordance with TLS BRs or GDCA's CP/CPS;
8. GDCA determines or is made aware that any of the information appearing in the certificate is inaccurate;
9. GDCA's right to issue certificates under the TLS BRs expires or is revoked or terminated, unless it has made arrangements to continue maintaining the CRL/OCSP repository;

10. The fulfillment of the obligations in the CP/CPS is delayed or encounters force majeure, such as natural disasters, computer or communications failures, changes of laws and regulations, government actions or other causes beyond the reasonable control, causing threats to the information of others;

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

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

1. 在任何 GDCA 得知证书中的域名或 IP 地址的使用不再被法律所允许的情形，如域名注册者使用域名的权利已被法院或仲裁机构撤销、与域名注册机构的合约终止、域名注册者更新域名失败等；
2. GDCA 得知一个通配符证书被用来验证一个欺诈性误导的子域名；
3. GDCA 由于某种原因终止运行，并且未安排其他 CA 提供撤销证书的支持性操作；
4. GDCA 签发证书的权利已届满或被撤销或终止，除非 GDCA 已做出安排，继续维护 CRL/OCSP；
5. 证书的技术内容或格式造成了对应用软件供应商或依赖方不可接受的风险。

If a certificate subscriber discovers or suspects that the security of the certificate private key has been compromised, the subscriber shall immediately notify GDCA to revoke the certificate. Revocation is also required if any of the following circumstances occur:

1. GDCA becomes aware that the use of the domain name or IP address contained in the certificate is no longer legally permitted, such as when the domain registrant's right to use the domain name has been revoked by a court or arbitral authority, the agreement with the domain name registrar has been terminated, or the domain registrant fails to renew the domain name;
2. GDCA becomes aware that a wildcard certificate has been used to authenticate a fraudulent or misleading subdomain;
3. GDCA ceases operations for any reason and has not arranged for another CA to provide certificate revocation support;
4. GDCA's authorization to issue certificates has expired, been revoked, or terminated, unless GDCA has made arrangements to continue maintaining CRL/OCSP services;
5. The technical content or format of the certificate presents an unacceptable risk to application software vendors or relying parties.

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

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

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

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

1. GDCA obtains evidence that the subordinate CA's private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with Sections 6.1.5 and 6.1.6 of the TLS BRs;
2. GDCA obtains evidence that the certificate was misused;
3. GDCA is made aware that the certificate was not issued in accordance with TLS BRs or that subordinate CA has not complied with the GDCA CP/CPS;
4. GDCA determines that any of the information appearing in the subordinate CA certificate is inaccurate, unreal or misleading;
5. GDCA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
6. GDCA's right to issue certificates under TLS BRs expires or is revoked or terminated, unless GDCA has made arrangements to continue maintaining the CRL/OCSP Repository.

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

请求证书撤销实体为订户、GDCA、经司法机构授权的司法人员。此外，依赖方、应用软件提供商、防病毒机构或其他的第三方可以提交证书问题报告，告知 GDCA 有合理理由撤销证书。

Entities authorized to request certificate revocation include the subscriber, GDCA, and judicial personnel authorized by judicial authorities. In addition, relying parties, application software providers, antivirus organizations, or other third parties may submit certificate problem reports to

inform GDCA of reasonable grounds for certificate revocation.

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

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

订户向 GDCA 提出证书撤销申请，GDCA 核实申请撤销实体的身份和授权实体的身份。

GDCA 提供 7*24 小时的证书撤销申请服务，订户可通过以下方式申请撤销：

- E-mail: webtrustreport@gdca.com.cn
- 电话号码：4007008088

GDCA 收到申请后 24 小时内处理撤销申请。

The subscriber submits a certificate revocation request to GDCA, and GDCA verifies the identity of the requesting entity and the authorized entity.

GDCA provides 24×7 certificate revocation request services. Subscribers may apply for revocation through the following methods:

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

GDCA shall process the revocation request within 24 hours after receipt of the application.

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

1. 当 GDCA 有本 CP/CPS 4.9.1.1 所述理由需要撤销订户的证书时，GDCA 的有关人员可以通过内部确定的流程提请撤销证书。
2. 在证书撤销后，GDCA 将通过适当的方式，包括邮件、电话等，通知最终订户证书已被撤销及被撤销的理由。若未能联络订户时，在必要的情况下，GDCA 对撤销的证书将通过网站进行公告。
3. GDCA 提供 7*24 小时的证书问题报告和处理流程。
4. 当依赖方、司法机构、应用软件提供商、防病毒机构等第三方发现证书可能存在问题，如私钥出现或怀疑出现泄漏、证书滥用、证书被用于可疑代码签名等，可及时通过以下方式进行问题报告：
   - E-mail: webtrustreport@gdca.com.cn
   - 电话号码：4007008088

GDCA 收到报告后，在 24 小时内对该证书问题报告内容进行调查，并基于以下标

准来决定是否撤销证书：

（1） 所报告问题的性质；

（2） 相应问题的出现次数和频率；

（3） 问题报告或投诉的实体；

（4） 用户对 GDCA CP/CPS 和订户协议等相关规范的遵循情况；

（5） 现行法律法规的遵循。

1. Where GDCA has grounds as described in Section 4.9.1.1 of this CP/CPS to revoke a subscriber's certificate, relevant personnel of GDCA may initiate a certificate revocation request in accordance with internally established procedures.

2. After a certificate has been revoked, GDCA will notify the subscriber of the revocation and the reasons for revocation through appropriate means, including email or telephone. If the subscriber cannot be contacted, GDCA may, where necessary, publish an announcement regarding the revoked certificate on its website.

3. GDCA provides 24×7 certificate problem reporting and handling procedures.

4. Where relying parties, judicial authorities, application software providers, antivirus organizations, or other third parties identify potential issues with a certificate—such as actual or suspected private key compromise, certificate misuse, or use of a certificate for signing suspicious code, they may promptly submit a certificate problem report through the following channels:

   - E-mail: webtrustreport@gdca.com.cn
   - Telephone: 4007008088

5. Upon receipt of a report, GDCA shall investigate the reported certificate issue within 24 hours and determine whether to revoke the certificate based on the following criteria:

   (1) the nature of the reported issue;

   (2) the number and frequency of occurrence of the issue;

   (3) the entity submitting the report or complaint;

   (4) the subscriber's compliance with GDCA CP/CPS, the Subscriber Agreement, and other applicable requirements;

   (5) compliance with applicable laws and regulations.

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

对于 GDCA 的根证书和中级证书，GDCA 根据本 CP/CPS 的规定决定是否撤销证书。

For GDCA root certificates and subordinate CA certificates, GDCA shall determine whether to revoke the certificates in accordance with the provisions of this CP/CPS.

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

如果出现密钥泄露或有泄露嫌疑等事件，撤销要求必须在发现泄密或有泄密嫌疑 8 小时以内提出。

In the event of a key compromise or suspected compromise, a revocation request must be submitted within eight hours of discovery of the compromise or suspected compromise.

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

GDCA 处理撤销请求的周期为 24 小时。

GDCA processes revocation requests within 24 hours.

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

GDCA 提供在线撤销状态查询，依赖方可在 GDCA 的网站上进行查询。

GDCA provides an online certificate revocation status checking service, and relying parties may perform such checks via the GDCA website.

4.9.7. CRL 发布频率 CRL Issuance Frequency

对于签发订户证书的 CA，GDCA 应至少每 7 天更新并发布一次 CRL，如有证书被撤销，应在记录该证书撤销状态后 24 小时内更新并发布新的 CRL。

对于签发中级 CA 证书的 CA，GDCA 须至少每 12 个月更新并发布一次 CRL，如有证书被撤销，应在记录该证书撤销状态后 24 小时内更新并发布新的 CRL。

For CAs issuing subscriber certificates, GDCA shall update and publish a new CRL at least every seven (7) days. If a certificate is revoked, GDCA shall update and publish a new CRL within twenty-four (24) hours after recording the certificate as revoked.

For CAs issuing subordinate CA certificates, GDCA shall update and publish a new CRL at least every twelve (12) months. If a certificate is revoked, GDCA shall update and publish a new CRL within twenty-four (24) hours after recording the certificate as revoked.

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

GDCA 的 CRL 发布最大滞后时间为发布周期之后的 24 小时内。

The maximum latency for GDCA CRL publication shall not exceed 24 hours after the end of the publication interval.

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

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

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

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

用户可以自由进行在线状态查询，GDCA 没有设置任何的读取权限。

GDCA 提供 Get 和 Post 两种方式的 OCSP 查询服务。

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

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

对于未签发的证书的状态查询请求，GDCA 不返回“good”状态。

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

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

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

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

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

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

GDCA 不提供撤销信息的其他发布形式。

GDCA does not provide any other forms of publication for revocation information.

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

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

证书订户以外的第三方可根据本 CP/CPS 的第 1.5.2 章中的联系方式，针对由 GDCA 签发的且未被撤销及未过期的证书，向 GDCA 发出证书密钥泄露的报告，报告方须使用以下方法之一证明持有或控制该证书对应的私钥：

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

GDCA 可酌情在本章节增加其他证明私钥泄露的方法。

Except for the circumstances specified in Section 4.9.1 of this CP/CPS, where a subscriber's certificate private key has been compromised or is suspected to have been compromised, the subscriber must promptly submit a certificate revocation request to GDCA.

A third party other than the certificate subscriber may, in accordance with the contact information provided in Section 1.5.2 of this CP/CPS, submit a key compromise report to GDCA regarding a certificate issued by GDCA that has not been revoked and has not expired. The reporting party shall demonstrate possession or control of the private key corresponding to the certificate by one of the following methods:

- submitting a CSR signed with the compromised private key, with “Proof of Key Compromise for GDCA” included in the Common Name (CN) field; or
- directly providing the compromised private key.

GDCA may, at its discretion, include additional methods in this section for demonstrating private key compromise.

4.9.13. 证书挂起的情形 Circumstances for Suspension

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

4.10.证书状态服务 Certificate Status Services

4.10.1.操作特征 Operational Characteristics

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

对于被撤销的证书，GDCA 在证书到期前不删除其在 CRL 中的撤销记录。

GDCA 不删除 OCSP 服务器中的撤销记录。

Subscribers may query certificate status via CRL, LDAP, and OCSP. The above certificate status services shall provide reasonable response times and adequate concurrent processing capability for query requests.

For revoked certificates, GDCA shall not remove their revocation records from the CRL prior to certificate expiration.

GDCA does not remove revocation records from the OCSP server.

4.10.2.服务可用性 Service Availability

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

GDCA provides 24×7 certificate status query services, with a response time not exceeding 10 seconds. Subject to network availability, subscribers are able to obtain certificate status information in real time.

4.10.3.可选特征 Operational Features

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

An additional optional method for certificate status checking is for subscribers to use the CRL distribution point designated by GDCA to query and download the CRL via a directory service, and

perform certificate status verification locally.

4.11.订购结束 End of Subscription

订购结束包含以下情况：

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

Termination of subscription includes the following circumstances:

1. When a subscriber ceases to use the certificate provided by GDCA, the subscriber must submit a certificate revocation request to GDCA. The application process shall follow the provisions of Section 4.9.3 of this CP/CPS. Upon revocation of the certificate by GDCA, the subscriber's subscription shall be deemed formally terminated.
2. When the certificate validity period expires and the subscriber fails to renew the service fee in a timely manner, the subscription shall be deemed formally terminated.
3. When the certificate expires and no certificate renewal or rekey is performed, the subscription shall be deemed formally terminated.

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

If a subscriber terminates the use of GDCA's certificate services during the certificate validity period, GDCA shall, upon approval of the termination request, revoke the subscriber's certificate in a timely manner and publish the revocation in accordance with the CRL publication policy. GDCA shall maintain detailed records of the revocation process and periodically archive the certificates and corresponding subscriber data following termination.

4.12.密钥生成、备份与恢复 Key Escrow and Recovery

GDCA 不托管任何证书订户的私钥，因此也不提供密钥恢复服务。

GDCA does not escrow any subscriber private keys and therefore does not provide key recovery services.

4.12.1. 密钥生成、备份与恢复的策略与行为 Key Escrow and Recovery Policy and Practices

不适用。

Not Applicable.

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

不适用。

Not Applicable.

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

5.1. 物理控制 Physical Controls

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

GDCA 的建筑物和机房建设按照下列标准实施：

- GB/T 25056-2018 《信息安全技术 证书认证系统密码及其相关安全技术规范》
- 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/T 2887-2011 《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》
- GB5054-2011 《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》

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

- GB/T 25056-2018 "Information Security Technology- Specifications of cryptograph

and the related security technology for certificate authentication system".

- GB/T39786-2021 "Information Security Technology-General Requirements for Information System Cryptography Application".
- GB50174-2017 "Design Code for Data Centers".
- GB/T36340-2018 "General Specification for Anti-static Access Floors".
- GB2887-2011 "Specification for computer field"
- GB50462-2024 "Code for Construction and Acceptance of Data Center Infrastructure".
- GB50222-2017 "Code for Fire Prevention in Design of Interior Decoration of Buildings".
- GB50116-2013 "Code for design of automatic fire alarm system"
- GB50057-2010 "Design code for protection of Structures against lightning"
- GB50054-2011 "Code for design of low voltage electrical installations"
- GB50019-2015 "Design Code for Heating, Ventilation and Air Conditioning of Industrial Buildings"

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

The GDCA data center is located in Shishan Town, Nanhai District, Foshan City. It is a standalone building equipped with earthquake resistance, fire protection, water protection, and lightning protection capabilities. There is only one entrance and access road to the data center building area. The GDCA central data center is functionally divided into five areas: the core area, service area, management area, operations area, and public area. Only authorized personnel are permitted to access their designated authorized areas.

5.1.1.1. 公共区域 Public Area

公共区包括入口、大堂、保安室，部署各类配套设施和监控设备。

The public area includes the entrance, lobby, and security room, and is equipped with supporting facilities and monitoring equipment.

5.1.1.2. 操作区 Operation Area

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

The operations area is the working area for RA personnel and management staff. Access to this area requires two-factor authentication, and all entry and exit activities shall be logged. From this level onward, all walls shall be constructed with high-strength protective materials.

5.1.1.3. 管理区 Management Area

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

The management area is equipped with RA management workstations, CA administration, issuance, and audit workstations, as well as network management and monitoring workstations. It serves as the working area for RA and CA administrators, auditors, and network security personnel. Access is restricted to authorized management personnel only, and entry requires two authorized administrators to jointly authenticate using two-factor authentication.

5.1.1.4. 服务区 Service Area

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

The service area primarily hosts equipment such as LDAP servers, OCSP servers, and RA registration servers. Access is restricted to authorized personnel designated for the service area, and entry requires two authorized administrators to jointly authenticate using two-factor authentication.

5.1.1.5. 核心区 Core Area

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

The core area is a shielded zone, equipped with high-strength steel security doors. It primarily houses critical equipment such as CA signing servers, CA database servers, KM key management servers, and timestamp servers. Access is restricted to authorized personnel designated for the core area, and entry requires two authorized administrators to jointly authenticate using two-factor authentication. A secure cabinet is also located in the core area for storing confidential materials.

5.1.2. 物理访问 Physical Access

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。

The GDCA data center is equipped with nine access-controlled doors fitted with electronic access control systems and one physical intrusion alarm system. The access control system is monitored in real time, enabling the retrieval of access records and the configuration of access permissions. The system can record entry and exit activities in real time and provides door-open timeout alarms. Personnel are required to use identification cards or a combination of identification cards and fingerprint authentication to gain access, and each door entry and exit is logged with timestamps and relevant information. Access to the service area and core area requires two administrators to jointly authenticate using identification cards and fingerprint verification. In accordance with standard data center operational procedures, access control records are compiled and archived on a monthly basis, and such records are retained for one year.

物理访问控制包括如下几个方面：

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

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

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

Physical access control includes the following aspects:

a) Access control system: Controls entry and exit through doors at each level. Personnel are required to use identification cards, or a combination of identification cards with passwords or fingerprint authentication, to gain access. Each entry and exit through any door shall be recorded with timestamps and relevant information.

b) Alarm system: Any abnormal events, such as unauthorized intrusion, forced door opening, or doors left open for an extended period, shall trigger the alarm system. The alarm system shall clearly indicate the location of the alarm.

c) Monitoring system: A video surveillance system is deployed in conjunction with the access control and physical intrusion alarm systems to provide 24×7 continuous recording of secure and operational areas. All video recordings shall be retained for at least six months for audit and reference purposes.

5.1.3. 安防监控 Security Monitoring

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

In accordance with the requirements of the data center power, environmental, and security monitoring system, the data center environmental monitoring system includes the following subsystems: power distribution monitoring subsystem, UPS monitoring subsystem, air conditioning equipment monitoring subsystem, fresh air system monitoring subsystem, temperature and humidity monitoring subsystem, water leakage detection subsystem, fire protection subsystem, access control subsystem, and video surveillance subsystem. These systems provide 24×7 real-time monitoring of infrastructure equipment, data center environmental conditions, and security system status. To support fault diagnosis and post-event auditing, monitoring records are retained for no less than six months.

5.1.4. 电力与空调 Power and Air Conditioning

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

The data center is powered by dual utility power supplies and one diesel generator, and is equipped with a dedicated power distribution room. Each data center area is equipped with independent power distribution equipment, as well as grounding and lightning protection systems. An uninterruptible power supply (UPS) system is deployed to provide power for more than eight hours. Anti-static measures are implemented within the data center to ensure equipotential bonding and grounding of cabinets, servers, and network equipment.

机房的空调采用风冷式冷凝器机组。机房按照 300kcal/h ㎡2 热负荷计算。夏季室外设计温度：35℃；冬季室外设计温度：0℃；机房室内设计温度：22±1℃，相对湿度：55±5%/h 。同时，机房安置了新风系统，对机房进行换气，保证机房内的空气品质和解决新风供应以及机房对空气清洁度的要求等问题。

The data center uses air-cooled condenser units. The data center is designed based on a heat load of 300 kcal/h·m². The outdoor design temperature is 35°C in summer and 0°C in winter. The indoor design temperature of the data center is maintained at 22±1°C, with a relative humidity of 55±5%. In addition, a fresh air system is installed to provide ventilation, ensuring indoor air quality, supplying fresh air, and meeting the data center’s air cleanliness requirements.

5.1.5. 水患防治 Water Exposures

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

To mitigate the risk of water damage to the data center, GDCA has installed a water leakage detection and alarm system within the air conditioning area. Water leakage detection cables are

deployed around the air conditioning units, and any leakage will immediately trigger an alarm to notify relevant personnel to take emergency measures. In addition, drainage channels and floor drains are installed along the perimeter of the exterior walls to ensure that any water can be promptly discharged. All external windows have been sealed to prevent water ingress.

5.1.6. 火灾防护 Fire Prevention and Protection

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

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

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。

All areas within the GDCA data center are equipped with smoke and heat fire detectors, as well as an automatic fire alarm system and an automatic gas-based fire suppression system. This system supports three activation modes: automatic, manual, and mechanical emergency operation.

In automatic mode, when a fire occurs in a protected area, the fire alarm control panel immediately issues a linkage signal upon receiving two independent fire alarm signals from that area. After a 30-second delay, the fire alarm control panel outputs a signal to activate the fire suppression system. At the same time, the control panel receives feedback from the pressure switch, and the door indicator lights in the protected area are activated to prevent personnel from entering inadvertently.

When personnel are frequently present in a protected area, the system can be switched from automatic mode to manual mode using the manual/automatic selector switch located outside the protected area. In the event of a fire under manual mode, the alarm control panel will only issue an alarm signal without initiating the suppression system. After confirmation of the fire by on-duty personnel, the system can be immediately activated by pressing the control panel or breaking the emergency activation button located outside the protected area, thereby discharging the gaseous extinguishing agent.

If both automatic and manual emergency activation fail, mechanical emergency activation can be performed within the cylinder storage room.

5.1.7. 介质存储 Media Storage

GDCA 对物理介质的存放和使用满足防火、防水、防震、防潮、防腐蚀、防虫害、

防静电、防电磁辐射等的安全需求。采取了介质使用登记注册、介质防复制及信息加密等措施实现了对介质的安全保护。

GDCA ensures that the storage and use of physical media meet security requirements for protection against fire, water, earthquakes, humidity, corrosion, pests, static electricity, and electromagnetic radiation. Measures such as media usage registration, anti-duplication controls, and information encryption are implemented to ensure the security of the media.

5.1.8. 废物处理 Waste Disposal

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

When archived paper documents and materials stored by GDCA are no longer required or have reached the end of their retention period, they shall be securely destroyed using measures that ensure the information cannot be recovered. Cryptographic devices and storage media containing sensitive information shall, prior to disposal, be initialized in accordance with the manufacturer's instructions and then physically destroyed.

5.1.9. 异地备份 Off-Site Backup

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

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

5.2. 程序控制 Procedural Controls

5.2.1. 可信角色 Trusted Roles

在 GDCA 提供的电子认证服务过程中，能从本质上影响证书的颁发、使用、管理和撤销等涉及密钥操作的职位都被 GDCA 视为可信角色。这些角色包括但不限于：密钥和密码设备的管理人员、系统管理人员、安全审计人员、业务管理人员及业务操作人员等，具体岗位名称和要求以 GDCA 的岗位说明为准。

In the process of providing electronic certification services, any role that can fundamentally affect key-related operations involving the issuance, use, management, and revocation of certificates is regarded by GDCA as a trusted role. Such roles include, but are not limited to, key and cryptographic device administrators, system administrators, security auditors, business managers, and operational personnel. Specific job titles and requirements shall be defined in GDCA's job descriptions.

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

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

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

GDCA strictly controls critical operations in its operational procedures. Sensitive operations require the joint participation of multiple trusted roles. For example:

1. Key and cryptographic device operations and storage: require the participation of 3 out of 5 trusted personnel.
2. Backend operations of the certificate issuance system: require the participation of 2 out of 3 system administrators classified as trusted personnel.
3. Certificate review and issuance: require the joint participation of 2 trusted personnel.

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

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

All personnel employed by GDCA who assume trusted roles shall undergo a defined vetting and verification process. The vetting procedures are specified in GDCA's personnel employment and management regulations.

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

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

a）证书业务受理

b）证书或 CRL 签发

c）系统工程与维护

d） CA 密钥管理

e）安全审计

To ensure system security, GDCA follows the principle of separation of trusted roles, whereby trusted roles are performed by different individuals. The roles subject to segregation of duties at GDCA include, but are not limited to, the following:

a) Certificate service application processing

b) Certificate or CRL issuance

c) System engineering and maintenance

d) CA key management

e) Security auditing

5.3. 人员控制 Personnel Controls

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

GDCA 对承担可信角色的工作人员的资格要求如下：

1. 具备良好的社会和工作背景。
2. 遵守国家法律、法规，服从 GDCA 的统一安排及管理。
3. 遵守 GDCA 有关安全管理的规范、规定和制度。
4. 具有良好的个人素质、修养以及认真负责的工作态度和良好的从业经历。
5. 具备良好的团队合作精神。
6. 无违法犯罪记录。
7. 关键和核心岗位的工作人员必须具备相关的工作经验，或通过 GDCA 相关的培训和考核后方能上岗。

GDCA's qualification requirements for personnel performing trusted roles are as follows:

1. Possess a good social and professional background.
2. Comply with national laws and regulations and adhere to GDCA's unified arrangements and management.
3. Comply with GDCA's security management standards, rules, and policies.
4. Demonstrate good personal qualities, integrity, a responsible working attitude, and relevant professional experience.
5. Possess strong teamwork spirit.
6. Have no criminal record.
7. Personnel in key and core positions must have relevant work experience or must pass GDCA-related training and assessments before being appointed.

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

GDCA requires that personnel performing trusted roles shall, at a minimum, possess loyalty, trustworthiness, and a strong commitment to their work, have no other part-time employment that

may affect CA operations, and have no record of significant professional misconduct in the industry.

5.3.2. 背景审查程序 Background Check Procedures

GDCA 或与有关的政府部门和调查机构合作，完成对可信员工的背景调查。

所有的可信员工和申请调入的可信员工都必须书面同意对其进行背景调查。背景调查必须符合法律法规的要求，调查内容、调查方式和从事调查的人员不得有违反法律法规的行为。背景调查应使用合法手段，尽可能地通过相关组织、部门进行人员背景信息的核实。

GDCA shall cooperate with relevant government authorities and investigative agencies to conduct background checks on trusted personnel.

All trusted personnel, as well as candidates applying for transfer into trusted roles, must provide written consent to such background checks. Background investigations shall comply with applicable laws and regulations. The content, methods, and personnel involved in the investigation shall not violate any laws or regulations. Background checks shall be conducted using lawful means and, where possible, through relevant organizations and authorities to verify personnel background information.

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。

Background checks are divided into basic checks and comprehensive checks.

Basic checks include verification of employment history, professional references, education, and social relationships.

Comprehensive checks include all items covered in basic checks, as well as verification of criminal records, social relationships, and public security-related matters.

调查程序包括：

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

b) 人事部门通过电话、网络等形式对其提供的材料的真实性进行鉴定。

c) 在背景调查中，对发现以下情形的人员，可以直接拒绝其成为可信人员的资格：

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

d) 完成调查后，GDCA 根据内部流程完成批准程序。

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

The investigation procedure includes the following:

a) The Human Resources department is responsible for verifying the personal information of applicants and collecting relevant supporting documents, including but not limited to resume, highest academic diploma, degree certificate, professional qualification certificates, and identification documents.

b) The Human Resources department shall verify the authenticity of the submitted materials through telephone calls, online verification etc.

c) During the background check process, candidates may be directly disqualified from trusted roles if any of the following conditions are identified:

- fabrication of facts or submission of false information;
- reliance on unreliable references;
- use of forged or illegal identity, education, or qualification documents;
- serious dishonest conduct in the workplace.

d) Upon completion of the investigation, GDCA shall complete the approval process in accordance with its internal procedures.

e) GDCA shall enter into a confidentiality agreement with the employee to ensure that all confidential and sensitive information related to CA certificate services is not disclosed. In addition, GDCA shall conduct ongoing job performance assessments of all personnel performing trusted roles in accordance with its personnel management regulations, in order to continuously verify their trustworthiness and job competence.

5.3.3. 培训要求 Training Requirements

GDCA 根据可信角色的职位需求，给予相应的岗前培训，综合培训内容如下：

- GDCA 运营体系；
- GDCA 技术体系；
- GDCA 安全管理策略和机制；
- 岗位职责统一要求；
- PKI 基础知识；
- 身份验证和审核策略和程序；
- 灾难恢复和业务连续性管理；

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

GDCA provides corresponding pre-employment training based on the requirements of trusted roles. The comprehensive training content includes, but is not limited to, the following:

- GDCA operational framework;
- GDCA technical framework;
- GDCA security management policies and mechanisms;
- Standardized job responsibilities;
- Fundamentals of PKI;
- Identity verification and validation policies and procedures;
- Disaster recovery and business continuity management;
- CP/CPS policies and related standards and procedures;
- GDCA management policies, rules, and procedures;
- National laws, regulations, standards, and procedures related to electronic certification services;
- Other necessary training as required.

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

GDCA will maintain records of employee training participation and archive such records. For operators and auditors involved in the issuance of SSL/TLS server certificates, successful completion of training and attainment of the skill level required by the TLS BRs for performing such duties shall be mandatory prior to assuming their roles.

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

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

Personnel performing trusted roles or other critical roles shall receive training organized by GDCA at least once per year. Personnel involved in the operation of certification systems shall receive at least one training session per year on relevant skills and knowledge. In addition, GDCA shall

require personnel to undergo ad hoc continuing training as needed in response to system upgrades, policy changes, and other organizational requirements.

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

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

The job rotation cycle and sequence for GDCA personnel shall be established in accordance with the organization's security management policies.

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

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

If any personnel are found to have used GDCA systems or performed certification operations without authorization or beyond their granted privileges, GDCA shall, upon confirmation, immediately revoke the individual's authentication certificate and terminate their system access rights. Depending on the severity of the unauthorized actions, GDCA may impose disciplinary measures including formal warnings, fines, dismissal, and referral to judicial authorities for further action.

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

GDCA 未聘用外部独立合约人从事认证相关的工作。

GDCA does not engage external independent contractors to perform certification-related activities.

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

在培训或再培训期间，GDCA 提供给员工的培训文档包括但不限于以下几类：

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

During training or retraining, GDCA provides employees with training documentation including, but not limited to, the following:

- GDCA Employee handbook;

- GDCA CP/CPS, and related agreements and specifications;
- GDCA technical system documentation;
- GDCA job responsibility descriptions;
- Internal operational documents, including business continuity management and disaster recovery plans;
- GDCA security management policies and procedures.

5.4. 审计日志程序 Audit Logging Procedures

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

所有发生在 GDCA 的重大安全事件会记录在审计跟踪档案中，可在必要时供合格审计师查看。这些记录，不论是手动生成或者是系统自动生成，都应该包含以下信息：

1. 事件发生的日期和时间；
2. 记录的序列号；
3. 记录的类型；
4. 记录的来源；
5. 记录事件的实体。

这些事件包括但不限于：

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

All significant security events occurring within GDCA shall be recorded in audit trail logs and made available to qualified auditors when necessary. These records, whether generated manually or automatically by the system, shall include the following information:

1. Date and time of the event;
2. Sequence number of the record;
3. Type of the record;
4. Source of the record;

Entity associated with the recorded event.

These events include, but are not limited to, the following:

1. Key lifecycle management events, including key generation, backup, storage, recovery, use, revocation, archival, destruction, and private key compromise;
2. Certificate lifecycle management events, including certificate application, approval, renewal, and revocation;
3. System and network security events, including successful and unsuccessful attempts to access CA systems, logs generated during routine system operations, and system changes;
4. Security events recorded via information security devices: Logging of router and firewall activities at a minimum include: 1) Successful and unsuccessful login attempts to routers and firewalls; and 2) Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and 3) Logging of all changes made to firewall rules, including additions, modifications, and deletions; and 4) Logging of all system events and errors, including hardware failures, software crashes, and system restarts.
5. System operation events, including the creation and deletion of system privileges, and the setting or modification of passwords;
6. Access to CA facilities, including records of authorized and unauthorized entry to CA facilities;
7. Trusted personnel management records, including the creation, deletion, and modification of system privileges.

5.4.2. 处理日志的周期 Frequency of Processing Log

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

GDCA conducts log tracking and review on a monthly basis to identify policy violations and other significant events, and performs log analysis of the certificate issuance system on a quarterly basis. All audit logs are regularly reviewed and examined by designated personnel to detect important security and operational events and to ensure that appropriate actions are taken in a timely manner.

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

GDCA 妥善保存电子认证服务的审计日志，在数据库保存审计日志至少两个月，保存期限不少于证书失效后五年。

GDCA shall securely retain audit logs associated with its electronic certification services. Such audit logs shall be stored in the database for a minimum of two months and retained for no less than five years after the associated certificates have expired.

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

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

GDCA's audit logs are stored in databases and are backed up, including audit information and event records documented in relevant materials. GDCA implements strict physical and logical access controls to ensure that only authorized personnel can access these audit records. Unauthorized access, reading, modification, or deletion is strictly prohibited.

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

GDCA 的审计跟踪文档由运维人员和审计人员每月进行审计日志和审计文档的归档备份。

GDCA's audit tracking documents are carried out by the operation and maintenance team and auditor for the archiving of audit log and audit documents monthly.

5.4.6. 审计收集系统 Audit Collection System

GDCA 的审计日志收集系统涉及：

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

GDCA's audit log collection system covers the following systems:

1. Certificate management system;
2. Certificate issuance system;
3. Certificate directory system;
4. Remote communication system;
5. Certificate application processing system;
6. Access control system;
7. Website and database security management systems;
8. Other systems subject to auditing as required.

GDCA 使用审计工具满足对上述系统审计的各项要求。

GDCA uses audit tools to meet the auditing requirements for the above-mentioned systems.

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

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

GDCA 有权决定是否对导致事件的实体进行通告。

If GDCA detects an attack, it will record the attacker's activities and, within the limits permitted by law, trace the attacker and reserve the right to take appropriate countermeasures. Depending on the nature of the attack, such measures may include terminating services provided to the attacker and referring the matter to judicial authorities.

GDCA reserves the right to determine whether to notify the entity responsible for the incident.

5.4.8. 脆弱性评估 Vulnerability Assessments

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

The CA security procedures are subject to vulnerability analysis in response to changes in policies, technologies, management practices, and significant system modifications. Identified weaknesses that can be remediated shall be promptly addressed, while those that cannot be remediated shall be managed appropriately. GDCA conducts annual vulnerability assessments of its systems to reduce operational risks.

5.5. 记录归档 Records Archival

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

GDCA 除归档本 CP/CPS 第 5.4.1 节相关记录外，还对以下几类事件进行归档记录，包括但不限于：

1. 与证书系统、证书管理系统、根 CA 系统安全有关的文档；
2. 与证书申请和证书验证、签发和撤销有关的文档。

In addition to retaining the records specified in Section 5.4.1 of this CP/CPS, GDCA shall archive records of the following types of events, including but not limited to:

1. Documents related to the security of the certificate system, certificate management system, and Root CA system;
2. Documents related to certificate application, certificate validation, certificate issuance, and certificate revocation.

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

对于本 CP/CPS 第 5.5.1 节所归档的记录，GDCA 将从该记录创建时间起至少保存 5 年。

GDCA shall retain the records archived pursuant to section 5.5.1 of this CP/CPS for a minimum period of five (5) years from the date such records are created.

5.5.3. 归档文件的保护 Protection of Archive

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

The protection of audit trail documentation is described in detail in the relevant sections below. Archival media are protected through physical security measures, and access is restricted to a strictly controlled entry point. Only GDCA management personnel are permitted to access these records.

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

对于系统生成的电子归档记录，每周进行备份，备份文件进行异地存放。对于书面的归档资料，不需要进行备份，但需要采取严格的措施保证其安全性。

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

止对档案及其备份进行删除、修改等操作。

For electronically generated archival records, backups shall be performed on a weekly basis, and backup files shall be stored off-site. For paper-based archival materials, backups are not required; however, strict measures shall be implemented to ensure their security.

All archived electronic files and databases are stored in GDCA's repository and are also backed up off-site. Archived databases are generally isolated through physical or logical separation and do not exchange information with external systems. Only authorized personnel, or personnel under their supervision, are permitted to access archival records. GDCA's security mechanisms ensure that deletion or modification of archival records and their backups is strictly prohibited.

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

GDCA 的所有日志都有时间记录，均由操作人员手工记录或系统自动添加。

All GDCA logs contain time records and are either manually recorded by operators or automatically generated by the system.

5.5.6. 归档收集系统 Archives Collection System

GDCA 的审计跟踪档案收集系统在本 CP/CPS 第 5.4 节中作详细说明。

The GDCA audit trail collection system is described in detail in Section 5.4 of this CP/CPS.

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

GDCA 采取了物理和逻辑的访问控制方法，以确保只有授权人员才能接近这些归档信息，严禁未授权的访问、阅读、修改和删除等操作。

GDCA implements both physical and logical access control measures to ensure that only authorized personnel can access archival information. Unauthorized access, reading, modification, and deletion are strictly prohibited.

5.6. 电子认证服务机构密钥的更替 Key Changeover

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

1. 在 CA 证书生命周期结束前停止签发新的下级证书，确保在 CA 的证书到期时所有下级证书也全部到期。
2. 在停止签发新的下级证书后至证书到期时，继续使用 CA 私钥签发 CRL，直到

最后一张下级证书过期。

3. 生成和管理 CA 密钥对时，严格遵守密钥规范。
4. 及时发布新的 CA 证书。
5. 确保整个过渡过程安全、顺利，不出现信任真空期。

Before certificate expiration, GDCA shall replace the root key in accordance with this CP/CPS and generate a new certificate. Key generation shall strictly comply with GDCA's key management specifications. CA key rollover shall follow the principles below:

1. No new subordinate certificates shall be issued before the end of the CA certificate lifecycle, ensuring that all subordinate certificates expire no later than the CA certificate.
2. After issuance of new subordinate certificates is stopped and until CA certificate expiration, the CA private key shall continue to be used to sign Certificate Revocation Lists (CRLs) until the last subordinate certificate has expired.
3. The generation and management of CA key pairs shall strictly comply with key management specifications.
4. The new CA certificate shall be published in a timely manner.
5. The entire transition process shall be secure and smooth, ensuring that no trust gap occurs.

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

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

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

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

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

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

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

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

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

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

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

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

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

The mass revocation plan includes the contents as required by section 5.7.1.2 of the TLS BRs.

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

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

GDCA maintains backups of resources, software, and data for business systems and other critical systems, and has established corresponding emergency handling procedures. In the event of damage to network communication resources, failure of computer equipment to provide normal services, software corruption, database tampering, or disasters caused by force majeure, GDCA will carry out recovery in accordance with its disaster recovery plan.

5.7.3. 实体私钥损害处理程序 Entity Private Key Compromise Procedures

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

1. 立即通知相关依赖方关闭与证书认证服务相关的系统。

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 GDCA 立即生成新的密钥对。
3. 新的根证书签发后，按照 CP/CPS 关于证书签发的规定，重新签发下级证书和下级操作中级 CA 证书。
4. GDCA 新的根证书签发后，将立即通过 GDCA 信息库、目录服务器、HTTP 等方式发布。

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

1. 立即进行内部汇报并生成新的密钥对和证书请求，申请签发新的证书。
2. 立即通知相关依赖方。
3. 立即撤销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。
4. 新的中级 CA 证书签发后，按照 CP/CPS 关于证书签发的规定，重新签发订户证书。
5. GDCA 新的中级证书签发后，将立即通过 GDCA 信息库、目录服务器、HTTP 等方式进行发布。

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

If a CA root private key is compromised, lost, tampered with, or disclosed, GDCA shall activate its major incident emergency response procedures. The Security Policy Committee and relevant experts shall conduct an assessment and formulate an action plan. If revocation of the CA certificate is required, the following measures shall be taken:

1. Relevant relying parties shall be immediately notified to shut down systems related to the certificate authentication services.
2. All issued certificates shall be immediately revoked, and CRL and OCSP information shall be updated for inquiry by certificate subscribers and relying parties. At the same time, GDCA shall immediately generate a new key pair.
3. After issuance of the new root certificate, subordinate certificates and subordinate operational intermediate CA certificates shall be reissued in accordance with the certificate issuance provisions of this CP/CPS.
4. Upon issuance of the new GDCA root certificate, it shall be immediately published through the GDCA repository, directory servers, HTTP, and other distribution methods.

If there is any suspicion that a subordinate CA private key has been lost, tampered with, compromised, disclosed, or misused by a third party, GDCA shall:

1. Immediately conduct internal reporting and generate a new key pair and certificate signing request (CSR) to apply for a new certificate.
2. Immediately notify relevant relying parties.
3. Immediately revoke all issued certificates and update CRL and OCSP information for inquiry by certificate subscribers and relying parties.
4. After issuance of the new intermediate CA certificate, subscriber certificates shall be reissued in accordance with the certificate issuance provisions of the CP/CPS.
5. Upon issuance of the new subordinate CA certificate, it shall be immediately published through the GDCA repository, directory servers, HTTP, and other distribution methods.

If a certificate subscriber's private key is suspected to have been damaged, lost, compromised, tampered with, or misused by a third party, the subscriber shall first apply for certificate revocation in accordance with the provisions of the GDCA CP/CPS, and shall then apply for a new certificate in accordance with the prescribed procedures.

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

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

Following the disasters described in Sections 5.7.1, 5.7.2, and 5.7.3, GDCA shall restore normal operations of all services within 24 hours through its backup mechanisms.

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

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

1. 委托业务承接单位；
2. 起草 GDCA 终止声明；
3. 通知与 GDCA 停止相关的实体；
4. 关闭从目录服务器；
5. 证书撤销；
6. 处理存档文件记录；
7. 停止认证中心的服务；
8. 存档主目录服务器；
9. 关闭主目录服务器；

10. 处理 GDCA 业务管理员和 GDCA 业务操作员的操作权限；
11. 处理和存储敏感文档；
12. 清除 GDCA 主机硬件。

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

The causes of GDCA termination may be categorized into key compromise-related causes and non-key compromise-related causes. Key compromise-related causes may include loss of the GDCA root key, while non-key compromise-related causes may relate to business considerations. Prior to the termination of GDCA operations, the following actions shall be completed:

1. Appoint a successor entity to assume the relevant services;
2. Prepare a GDCA termination statement;
3. Notify entities affected by the termination of GDCA operations;
4. Shut down subordinate directory servers;
5. Revoke certificates;
6. Process archived records and files;
7. Terminate certification authority services;
8. Archive the primary directory server;
9. Shut down the primary directory server;
10. Revoke or otherwise handle the operational privileges of GDCA business administrators and operators;
11. Process and securely store sensitive documents;
12. Sanitize or dispose of GDCA host hardware.

Termination of GDCA operations due to key compromise-related causes or non-key compromise-related causes generally requires substantially the same procedures. The primary difference lies in the timing requirements for notifications issued upon termination.

Where termination is caused by key compromise-related reasons, GDCA will complete the process of notifying subscribers as promptly as possible. Where termination is caused by non-key compromise-related reasons, GDCA will, after notifying all subscribers, take appropriate measures to mitigate the impact of the termination on subscribers.

6. 认证系统技术安全控制 Technical Security Controls

6.1. 密钥对的生成与安装 Key Pair Generation and Installation

6.1.1. 密钥对的生成 Key Pair Generation

6.1.1.1. CA 密钥对生成 CA Key Pair Generation

CA 密钥对必须在安全的物理环境中，由多个可信人员在国家密码主管部门批准和许可的密码设备中生成。密钥的生成、管理、存储、备份和恢复应遵循 FIPS140-2 标准的相关规定。

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/CPS 以及角色分离的要求。密钥对生成过程和操作均需记录并保存。

CA key pairs shall be generated within a secure physical environment by multiple trusted personnel using cryptographic devices approved and licensed by the national cryptographic authority. The generation, management, storage, backup, and recovery of keys shall comply with the relevant requirements of the FIPS 140-2 standard.

The CA key pair generation process shall be video recorded or witnessed by a qualified auditor to ensure compliance with the CP/CPS and the requirements for separation of duties. The key pair generation process and related operations shall be documented and retained.

6.1.1.2. 订户密钥对生成 Generation for Subscriber Key Pair

订户的密钥对由订户自己生成并保管，证书订户负有保护私钥安全的责任和义务，并承担由此带来的法律责任。

在公钥对应于行业公认的弱私钥方面，GDCA 至少应采取以下预防措施：

1.对于 Debian 弱密钥漏洞（https://wiki.debian.org/SSLkeys），GDCA 拒绝在 https://github.com/cabforum/Debianweak-keys/ 中列出的每种密钥类型（例如 RSA、ECDSA）和密钥长度的所有密钥。对于满足第 6.1.5 节要求的其他密钥，除 RSA 密钥长度超过 8192 位的情况外，GDCA 拒绝 Debian 弱密钥。

2.对于 ROCA 漏洞，GDCA 拒绝通过 https://github.com/crocs-muni/roca 或等效工具识别的密钥。

3.对于接近素数漏洞（https://fermatattack.secvuln.info/），GDCA 拒绝可通过 Fermat 分解方法在 100 轮内分解的弱密钥。

The subscriber key pair shall be generated and maintained by the subscriber. The certificate

subscriber shall be responsible for protecting the security of the private key and shall bear the corresponding legal liabilities arising therefrom.

With respect to public keys corresponding to industry-recognized weak private keys, at least the following precautions shall be implemented by GDCA:

1. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), GDCA shall reject all keys found at https://github.com/cabforum/Debianweak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of Section 6.1.5, with the exception of RSA key sizes greater than 8192 bits, GDCA shall reject Debian weak keys.

2. In the case of ROCA vulnerability, GDCA shall reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.

3. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), GDCA shall reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

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

GDCA 不需要将私钥传递给订户。

GDCA does not deliver private keys to subscribers.

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

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

Subscribers shall electronically submit public keys to GDCA for certificate issuance through certificate signing requests (CSRs) in PKCS#10 format or through other digitally signed file package formats. Prior to certificate issuance, GDCA shall verify the subscriber signature contained in the submitted request.

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

GDCA 的公钥包含在 GDCA 自签发的根 CA 证书和中级 CA 证书中，通过 GDCA 官方网站进行发布，以供证书订户和依赖方查询使用。

GDCA's public key is included in the self-signed root CA certificate and subordinate CA certificates issued by GDCA, and is published on the official GDCA website for inquiry and use by certificate subscribers and relying parties.

6.1.5. 密钥的长度 Key Sizes

GDCA 支持的 RSA 密钥长度为 2048 位或以上（位数能被 8 整除），支持的 ECC 密钥长度为 256 或以上。

GDCA supports RSA key lengths of 2048 bits or greater (with bit lengths divisible by 8), and supports ECC key lengths of 256 bits or greater.

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

对于参数质量的检查，GDCA 使用遵循 FIPS140-2 规定的加密设备和生成和存储密钥，已经具备足够的安全等级要求。

For parameter quality verification, GDCA uses cryptographic devices that comply with FIPS 140-2 requirements for key generation and storage, thereby meeting the required security level.

6.1.7. 密钥使用目的（基于 X.509 v3 密钥用途字段）Key Usage Purposes (as per X.509 v3 Key Usage Field)

GDCA 的根 CA 密钥仅用于签署以下证书：

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

Private keys corresponding to GDCA root certificates are used to sign the following certificates only:

1. The self-signed certificate representing the root CA;
2. Certificates for cross-certificates of subordinate CA certificates;
3. Certificates used for infrastructure purposes (e.g., OCSP responder verification certificates).

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

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

GDCA 用于 CA 密钥对的密码模块符合 FIPS 140-2 第三级别的技术要求。

The cryptographic modules used by GDCA for CA key pairs comply with the technical requirements of FIPS 140-2 Level 3.

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

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

Activities involving GDCA private keys, including generation, renewal, revocation, backup, and recovery, are subject to a multi-person control mechanism. Specifically, a “three-out-of-five” control scheme is implemented, whereby private key management authority is distributed among five key custodians. Private key activities may only be performed when at least three custodians are present and authorized, with administrator cards inserted and corresponding PIN codes entered.

6.2.3. 私钥托管 Private Key Escrow

GDCA 不对订户私钥进行托管。

GDCA does not provide escrow services for subscriber private keys.

6.2.4. 私钥备份 Private Key Backup

GDCA 对根私钥和 CA 私钥进行备份，按照加密设备制造商提供的操作规范生成备份密文文件和备份恢复介质，在多地理位置以多点存放方式进行本地和异地备份，并在多人控制机制下进行管理。

GDCA performs backups of root private keys and CA private keys. Backup encrypted files and backup recovery media are generated in accordance with the operational procedures provided by the cryptographic device manufacturer. Backups are stored both on-site and off-site an in multiple geographic locations, under multi-person control.

6.2.5. 私钥归档 Private Key Archival

GDCA 不对私钥进行归档存储。

GDCA does not archive private keys.

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

所有的密钥都必须在密码模块中产生，密码模块中的私钥不能以明文的形式导出。

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

All keys shall be generated within cryptographic modules, and private keys within the cryptographic modules shall not be exported in plaintext form.

For CA systems, where backup or migration of CA keys is required, keys exported from the cryptographic modules shall be encrypted. The private keys used to encrypt CA keys shall be subject to multi-person control. Restoration of backed-up keys into cryptographic modules shall also be performed under multi-person control.

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

CA 系统的密码设备采用国家密码管理局批准和许可的服务器密码机，硬件密码模块至少符合 FIPS 140-2 三级标准或同等级安全水平，私钥的数据存储在服务器密码机硬件中，在整个生命周期都不会明文出现在硬件密码机之外。

The cryptographic devices used in the CA system are server cryptographic modules approved and licensed by the State Cryptography Administration. The hardware cryptographic modules at least meet the FIPS 140-2 level 3 standards or equivalent security levels. Private key data are stored within the server cryptographic hardware and shall not appear in plaintext outside the hardware cryptographic modules throughout their entire lifecycle.

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

GDCA 的 CA 私钥存放在硬件密码模块中，激活需按本 CP/CPS 第 6.2.2 节，在三名密钥管理员在场并许可的情况下，使用加密设备的操作员权限实现。

GDCA's CA private keys are stored within hardware cryptographic modules. Activation shall be performed in accordance with Section 6.2.2 of this CP/CPS. It requires the presence and authorization of three key custodians, and shall be carried out using the operator privileges of the cryptographic device.

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

解除 CA 私钥激活状态的操作，在三名密钥管理员在场并许可的情况下，由密钥管理员使用含有自己的管理员卡登录服务器密码机，进行解除私钥的操作。

GDCA 解除私钥激活状态的方式包括退出登陆状态、切断电源、将硬件密码模块移开、注销用户或系统等。未经授权的任何人员，绝不可以进行相关操作。

The deactivation of a CA private key shall be performed in the presence and with the authorization of three key custodians. Key custodians shall log in to the server cryptographic module using their respective administrator cards to carry out the private key deactivation operation.

GDCA's methods for deactivating private keys include, but are not limited to, logging out of the system, disconnecting the power supply, removing the hardware cryptographic module, or terminating user or system sessions. Any unauthorized personnel are strictly prohibited from performing such operations.

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

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

If a CA private key is no longer in use, or if the public key corresponding to the private key has expired or been revoked, the following measures shall apply: where the private key resides within a software cryptographic module, the module shall be securely erased by overwriting; where the private key resides within a hardware cryptographic module, the cryptographic device, IC card, or equivalent medium shall be zeroized. In addition, all PIN codes, IC cards, and other activation materials used to activate the private key shall also be destroyed or retrieved.

6.2.11. 密码模块的评估 Cryptographic Module Rating

参考本 CP/CPS 第 6.2.1 节。

See section 6.2.1 of this CP/CPS.

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

6.3.1. 公钥归档 Public Key Archival

参考本 CP/CPS 第 5.5 章。

See section 5.5 of this CP/CPS.

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

在 2026 年 3 月 15 日之前签发的 SSL/TLS 服务器证书，其有效期不应超过 397 天，且不得超过 398 天。2026 年 3 月 15 日当天及之后且在 2027 年 3 月 15 日之前签发的 SSL/TLS 服务器证书，其有效期不应超过 199 天，且不得超过 200 天。2027 年 3 月 15 日当天及之后且在 2029 年 3 月 15 日之前签发的 SSL/TLS 服务器证书，其有效期不应超过 99 天，且不得超过 100 天。2029 年 3 月 15 日当天及之后签发的 SSL/TLS 服务器证书，其有效期不应超过 46 天，且不得超过 47 天。SSL/TLS 服务器证书最长有效期参考下表：

证书颁发日期当天或之后	证书颁发日期在当天之前	证书最大有效期
	2026 年 3 月 15 日	398 天

2026 年 3 月 15 日	2027 年 3 月 15 日	200 天
2027 年 3 月 15 日	2029 年 3 月 15 日	100 天
2029 年 3 月 15 日		47 天

SSL/TLS server certificates issued before 15 March 2026 should not have a validity period greater than 397 days and must not have a validity period greater than 398 days. SSL/TLS server certificates issued on or after 15 March 2026 and before 15 March 2027 should not have a validity period greater than 199 days and must not have a Validity Period greater than 200 days. SSL/TLS server certificates issued on or after 15 March 2027 and before 15 March 2029 should not have a validity period greater than 99 days and must not have a validity period greater than 100 days. SSL/TLS server certificates issued on or after 15 March 2029 should not have a validity period greater than 46 days and must not have a validity period greater than 47 days. The maximum validity period for SSL/TLS server certificates is shown in the table below:

Certificate issued on or after	Certificate issued before	Maximum validity period
	March 15, 2026	398 days
March 15, 2026	March 15, 2027	200 days
March 15, 2027	March 15, 2029	100 days
March 15, 2029		47 days

6.4. 激活数据 Activation Data

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

CA 私钥的激活数据，必须按照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。

Activation data for CA private keys shall be generated, distributed, and used in strict accordance with the applicable requirements for activation data splitting and key management procedures.

Subscriber private key activation data, including certificate download passwords, USB Key PINs, IC card login passwords, and similar credentials, shall be randomly generated within a secure and reliable environment.

6.4.2. 激活数据的保护 Activation Data Protection

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

订户的激活数据必须在安全可靠的环境下产生，必须进行妥善保管，或者记住以后

进行销毁，不可被他人所获悉。

Activation data for CA private keys shall be securely split using reliable methods and entrusted to different trusted personnel. Such custodians shall comply with the requirements for separation of duties.

Subscriber activation data shall be generated within a secure and reliable environment and shall be properly protected. After being memorized, such activation data shall be destroyed and shall not be disclosed to any unauthorized party.

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

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

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

When private key activation data are transmitted, they shall be protected against loss, theft, modification, unauthorized disclosure, and unauthorized use during transmission.

When private key activation data are no longer needed, they shall be destroyed in a manner that protects them against theft, disclosure, or unauthorized use during the destruction process. The destruction method shall ensure that none of the activation data, in whole or in part, can be directly or indirectly recovered from residual information or media. For example, paper records containing passwords shall be shredded.

6.5. 计算机安全控制 Computer Security Controls

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

GDCA 系统的信息安全管理，按照国标《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。

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

通过严格的安全控制手段，确保 CA 软件和数据文件的系统是安全可信的系统，不会受到未经授权的访问。

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。

GDCA's information security management system is established and implemented in accordance with the national standard Information Security Technology - Cryptographic and Related Security Technical Specifications for Certificate Authentication Systems, the Administrative Measures for Electronic Certification Services issued by the Ministry of Industry and Information Technology, with reference to the ISO 27001 information security standard and other relevant information security standards. GDCA has developed comprehensive and well-defined security management policies and procedures, which are implemented, reviewed, and documented during operations. Major security technologies and control measures include identity identification and authentication, logical access control, physical access control, separation of personnel duties, and network access control.

A strict two-factor authentication mechanism is enforced. Each individual with access privileges to the systems (including CA systems and RA systems) is assigned a unique account, and account permissions are restricted to the minimum privileges necessary to perform job responsibilities. Access requires two-factor authentication using a username, password, and digital certificate.

Through strict security control measures, GDCA ensures that the systems hosting CA software and data files are secure and trustworthy and are protected against unauthorized access.

Core systems shall be physically separated from other systems, and production systems shall be logically isolated from other systems. Such separation prevents network access except through designated applications. Firewalls are used to prevent intrusions into production system networks from both internal and external networks and to restrict activities accessing production systems. Only trusted personnel within the CA system operations and management group who have a legitimate business need may access the CA database using authorized credentials.

6.5.2. 计算机安全评估 Computer Security Rating

GDCA 建立并实施信息安全管理制度，对认证系统、计算机系统及网络环境进行持续的安全管理和风险控制。

GDCA establishes and implements an information security management system to ensure the continuous security management and risk control of its certification systems, computer systems, and network environment.

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

6.6.1. 系统开发控制 System Development Controls

GDCA 的软件设计和开发过程遵循以下原则：

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

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

GDCA's software design and development processes follow the principles below:

1. Establishing internal upgrade and change request procedures and requiring personnel to strictly comply with the prescribed processes;
2. Establishing internal procurement procedures and management policies;
3. Requiring all software applications to undergo rigorous testing in the development environment before deployment to the production environment;
4. Performing effective online backups prior to change deployment;
5. Conducting third-party verification and review;
6. Performing security risk analysis and reliability-oriented design.

In addition, GDCA's software development and operational procedures are implemented with reference to the ISO/IEC 15408 standard and related planning and development controls.

6.6.2. 安全管理控制 Security Management Controls

GDCA 认证系统的信息安全管理，严格遵循国家密码管理局的有关运行管理规范进行操作。

GDCA 认证系统的使用具有严格的控制措施，所有的系统都经过严格的测试验证后才进行安全和使用，任何修改和升级会记录在案并进行版本控制、功能测试和记录。GDCA 还对认证系统进行定期和不定期的检查和测试。

GDCA 采用一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。

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。

The information security management of GDCA certification systems is operated in strict accordance with the relevant operational management requirements issued by the State Cryptography Administration.

The use of GDCA certification systems is subject to strict control measures. All systems undergo rigorous testing and verification before being approved for secure operation and use. Any modifications and upgrades are documented and subject to version control, functional testing, and record retention. GDCA also conducts periodic and ad hoc inspections and testing of its certification systems.

GDCA adopts a flexible management framework to control and monitor system configurations in order to prevent unauthorized modifications.

Hardware devices are subject to security inspections upon procurement and receipt to identify potential compromises, intrusions, or security vulnerabilities. The procurement and installation of cryptographic devices are conducted under enhanced security control mechanisms, including device inspection, installation, and acceptance procedures.

Following upgrades of hardware and software equipment within GDCA certification systems, obsolete equipment shall, prior to disposal, be examined to determine whether any security-sensitive information remains stored on the devices.

6.6.3. 生命周期的安全控制 Life Cycle Security Controls

GDCA 认证系统的软硬件设备具备可持续性的升级计划，其中包括了对软、硬件生命周期的安排。

The hardware and software equipment of the GDCA certification systems are subject to sustainable upgrade plans, including lifecycle management arrangements for both hardware and software components.

6.7. 网络的安全控制 Network Security Controls

GDCA 认证系统采用多级防火墙和网络资源安全控制系统的保护，并且实施完善的访问控制技术。

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

为了确保网络安全，GDCA 认证业务系统安装部署了入侵检测、安全审计、防毒防

范和网管系统，并且及时更新防火墙、入侵监测、安全审计、防病毒和网管系统的版本，以尽可能的降低来自于网络的风险。

GDCA 的网络安全控制符合 CA/浏览器论坛（CA/Browser Forum）发布的 Network and Certificate System Security Requirements（NCSSR）的要求。

GDCA 至少每季度执行一次网络漏洞扫描，漏洞响应及整改时间表根据漏洞严重程度确定，关键漏洞需在 96 小时内完成响应及整改，高/中危漏洞需在 60 天内响应及整改。对于例外情况，GDCA 应进行记录、风险评估并存档。

GDCA certification systems are protected through multi-layer firewalls and network resource security control systems, and comprehensive access control technologies are implemented.

The certification systems expose only operational functions related to certificate application, certificate inquiry, and similar services for user access through the network. Only personnel authorized by GDCA are permitted to access devices or systems such as the GDCA certificate servers, GDCA certificate directory servers, and GDCA operations center.

To ensure network security, GDCA certification business systems are equipped with intrusion detection systems, security audit systems, anti-malware protection systems, and network management systems. In addition, GDCA timely updates the versions of its firewall, intrusion detection, security audit, anti-malware, and network management systems in order to minimize network-related risks to the greatest extent possible.

The network controls adopted by GDCA conform to the Network and Certificate System Security Requirements (NCSSR）published by the CA/Browser Forum.

Vulnerability scans of networks are performed at least once a quarter by GDCA. Responding and remediation timelines are governed by severity, with critical vulnerabilities addressed within 96 hours and high/medium vulnerabilities resolved within 60 days. Exceptions are documented, assessed for risk, and recorded.

6.8. 时间戳 Time-Stamping

见本 CP/CPS 第 5.5.5 节。

See section 5.5.5 of this CP/CPS.

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

7.1. 证书 Certificate Profile

GDCA 签发的证书符合 ITU-T X.509v3 和 RFC 5280：Internet X.509 公钥基础设施证书和 CRL 结构。GDCA 通过 CSPRNG 生成大于 0 且长度为 64 位的非序列性的证书

序列号。

Certificates issued by GDCA comply with ITU-T X.509 Version 3 and Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. GDCA generates non-sequential certificate serial numbers greater than zero containing 64 bits of output from a CSPRNG.

GDCA 所签发证书结构基本域如下：

域	值或值的限制
版本	指明 X.509 证书的格式版本，值为 V3
序列号	证书的唯一标识符
签名算法	签发证书时所使用的签名算法（见 CP/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 DV SSL 证书 DN：CN。 订户 OV SSL 证书 DN：CN、O、L、S、C。 订户 EV SSL 证书 DN：CN、O、streetAddress（可选）、postalCode（可选）、L、S、C、serialNumber、businessCategory、jurisdictionLocalityName（OID：1.3.6.1.4.1.311.60.2.1.1）、jurisdictionStateOrProvinceName（OID:1.3.6.1.4.1.311.60.2.1.2）、jurisdictionCountryName（OID:1.3.6.1.4.1.311.60.2.1.3）。
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。

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

Fields	Value or value limit
Version	The format version of X.509 certificate with a value of V3.
Serial Number	The unique identifier of a certificate.
Signature Algorithm	The signature algorithm used to issue certificates (Section 7.1.3 of this CP/CPS).
Issuer	Issuer's distinguished name, including CN, O, and C.

notBefore	Based on Coordinated Universal Time (UTC), synchronized with Beijing time, encoded according to RFC 5280.
notAfter	Based on Coordinated Universal Time (UTC), synchronized with Beijing time, encoded according to RFC 5280.
Subject	Subject DN of a certificate holder or entity may be as follows: DN of a root CA certificate: CN, O, C. DN of a subordinate CA certificate: CN, O, C. DN of a subscriber DV SSL certificate: CN. DN of a subscriber OV SSL certificate: CN, O, L, S, C. DN of a subscriber EV SSL certificate：CN, O, streetAddress (Optional), postalCode (Optional), L, S, C, SerialNumber, businessCategory, jurisdictionLocalityName (OID:1.3.6.1.4.1.311.60.2.1.1), jurisdictionStateOrProvinceName (OID:1.3.6.1.4.1.311.60.2.1.2), jurisdictionCountryName (OID:1.3.6.1.4.1.311.60.2.1.3).
Public key	Encoded according to RFC 5280, using the algorithms specified in section 7.1.3 of this CP/CPS, with key sizes meeting requirements specified in this CP/CPS.

7.1.1. 版本号 Version Number(s)

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

GDCA certificates conform to the X.509 Version 3 certificate format, and version information is contained within the certificate version field.

7.1.2. 证书扩展项 Certificate Extensions

GDCA 签发的证书扩展项遵循 X.509 V3 证书标准。不同类型证书的扩展项定义见后续章节。

Certificate extensions in certificates issued by GDCA conform to the X.509 Version 3 certificate standard. Extension for different certificate types is provided in the following sections.

7.1.2.1. 根证书 Root CA Certificate

1. 基本约束

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

2. 密钥用法

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

3. 证书策略

该扩展项未设置。

4. 增强型密钥用法

该扩展项未设置。

5. 主题密钥标识符

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

7. basicConstraints

This extension shall appear and shall be marked critical. The cA field shall be set true, and the pathLenConstraint field is not present.

8. keyUsage

This extension shall be present and shall be marked critical. The usage keyCertSign and cRLSign shall be set. The private key corresponding to a Root CA will not be used for signing OCSP responses.

9. certificatePolicies

This extension is not set for root CA certificates.

10. extKeyUsage

This extension is not set for root CA certificates.

11. subjectKeyIdentifier

This extension shall be present and shall not be marked critical. It shall contain a value that is included in the keyIdentifier field of the authorityKeyIdentifier extension in certificates issued by the Root CA.

7.1.2.2. 中级 CA 证书 Subordinate CA Certificate

1. 证书策略

中级 CA 证书中须设置该扩展项，且不得为关键扩展项，有关具体的策略标识符的信息请见本 CP/CPS 的第 1.4.1.2 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 证书应设有颁发机构信息访问扩展项，且不得为关键扩展项。此扩展中会

包含指向此 CA 证书签发者证书的 HTTP 地址（AccessMethod=1.3.6.1.5.5.7.48.2）和指向 CA OCSP 服务的 HTTP 地址（AccessMethod=1.3.6.1.5.5.7.48.1）。

4. 基本约束

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

5. 密钥用法

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

6. 增强型密钥用法

对于在 2019 年 1 月 1 日后签发的中级 CA 证书，中级 CA 证书中须设置该扩展项，且不应为关键扩展项，若该类中级 CA 证书将被用于签发 SSL/TLS 证书，则该扩展项须含 id-kp-serverAuth【RFC5280】，可包含 id-kp-clientAuth【RFC5280】，不得包含 id-kpemailProtection【RFC5280】，id-kp-codeSigning【RFC5280】，id-kptimeStamping【RFC5280】，id-kp-OCSPSigning【RFC5280】及 anyExtendedKeyUsage【RFC5280】，也不得包含任何其他值。

7. 颁发机构密钥标识符

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

8. 主题密钥标识符

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

1. certificatePolicies

This extension for subordinate CA certificates shall be present and shall not be marked critical. More information about the asserted OIDs is explained in section 1.4.1.2 of this CP/CPS.

2. cRLDistributionPoints

This extension for subordinate CA certificates shall be present and shall not be marked critical. It shall contain the HTTP URL of the CA’s CRL service.

3. authorityInformationAccess

For subordinate CAs certificates, this extension should be present and shall not be marked critical. It should contain the HTTP URL of the Issuing CA’s certificate (accessMethod = 1.3.6.1.5.5.7.48.2). It may contain the HTTP URL of the Issuing CA’s OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

4. basicConstraints

This extension for subordinate CA certificates shall be present and shall be marked critical. The cA field shall be set true. The pathLenConstraint field may be present.

5. keyUsage

The subordinate CA certificates have the "keyUsage" extension, which is a critical extension. Usage settings are: digitalSignature, keyCertSign, cRLSign. The private key corresponding to a subordinate CA certificate will not be used for signing OCSP responses.

6. extKeyUsage

For subordinate CA certificates issued after 1 January 2019, this extension shall be present and should not be marked critical. If such subordinate CA certificates will be used to issue SSL/TLS certificates, the value id-kp-serverAuth [RFC5280] shall be present. The value id-kp-clientAuth [RFC5280] may be present. The values id-kpemailProtection [RFC5280], id-kp-codeSigning [RFC5280], id-kptimeStamping [RFC5280], id-kp-OCSPSigning [RFC5280] and anyExtendedKeyUsage [RFC5280] shall not be present. Other values should not be present.

7. authorityKeyIdentifier

This extension for subordinate CA certificates shall be present and shall not be marked critical. This extension contains only the "KeyIdentifier" field.

8. subjectKeyIdentifier

This extension shall be present and shall not be marked critical. It shall contain a value that is included in the keyIdentifier field of the authorityKeyIdentifier extension in certificates issued by the subordinate CA.

7.1.2.3. 订户证书 Subscriber Certificate

1. 证书策略

订户证书中须设置该扩展项，且不得为关键扩展项，有关具体的策略标识符的信息请见本 CP/CPS 的第 1.4.1.2 节。

2. CRL 分发点

订户证书须设置该扩展项项，且此扩展项为非关键扩展。此扩展项中会包含指向 CA CRL 服务的 HTTP URL 地址。

3. 颁发机构信息访问

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

4. 基本约束

可设置该扩展项，若设置，则该扩展项须为关键扩展项，此扩展中“cA”字段须设置为“False”。

5. 密钥用法

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

6. 增强型密钥用法

订户证书中的密钥用法及增强型密钥用法如下：

DV SSL 证书	密钥用法：数字签名，密钥加密。 增强型密钥用法：服务器身份验证。
OV SSL 证书	密钥用法：数字签名，密钥加密。 增强型密钥用法：服务器身份验证。
EV SSL 证书	密钥用法：数字签名，密钥加密。 增强型密钥用法：服务器身份验证。

7. 颁发机构密钥标识符

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

8. 主题密钥标识符

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

1. certificatePolicies

This extension for subscriber certificates shall be present and shall not be marked critical. More information about the asserted OIDs is explained in section 1.4.1.2 of this CP/CPS.

2. cRLDistributionPoints

This extension shall be present and shall not be marked critical. It shall contain the HTTP URL of the CA's CRL service.

3. authorityInformationAccess

This extension shall be present and shall not be marked critical. This extension will contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2) and the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

4. basicConstraints

This extension may be present and shall be marked critical if present, and the cA field shall be set

to "False" if present.

5. keyUsage

This extension for subscriber certificates may be present, and if present, usage keyCertSign and cRLSign shall not be set.

6. extKeyUsage

Key usage and extended key usage are as follows:

Types of Certificates	**Key Usages**
DV SSL Certificates	KU: Digital Signature, Key Encipherment. EKU: Server Authentication.
OV SSL Certificates	KU: Digital Signature, Key Encipherment. EKU: Server Authentication.
EV SSL Certificates	KU: Digital Signature, Key Encipherment. EKU: Server Authentication.

7. authorityKeyIdentifier

This extension for subscriber certificates shall be present and shall not be marked critical. This extension contains only the "KeyIdentifier" field.

8. subjectKeyIdentifier

This extension shall be present and shall not be marked critical. It shall contain a value that is included in the keyIdentifier field of the authorityKeyIdentifier extension in certificates issued by the subordinate CA.

7.1.2.4. 所有证书 All Certificates

GDCA 签发的所有证书均符合 RFC5280，对于中级 CA 证书以及订户证书，密钥用法、增强型密钥用法及证书扩展项均符合本 CP/CPS 第 7.1.2.2、及 7.1.2.3 的要求。

For the subscriber certificates and subordinate CA certificates, key usages, extended key usages and certificate extensions conform to section 7.1.2.2, and 7.1.2.3 of this CP/CPS.

7.1.2.5. RFC5280 的应用 Application of RFC 5280

为澄清起见，RFC 6962 定义的“预证书”不被视为 RFC5280 定义的“证书”。

For purposes of clarification, a precertificate, as described in RFC 6962 shall not be considered to be a “certificate” subject to the requirements of RFC 5280.

7.1.3. 算法对象标识符 Algorithm Object Identifiers

GDCA 签发的数字证书使用以下相关算法之一：

sha256RSA withRSAEncryption	1.2.840.113549.1.1.11
SHA256 with ECDSA	1.2.840.10045.4.3.2

中级 CA 证书、订户证书、及 OCSP 证书的密码算法不使用 sha1RSA。

GDCA uses one of the following relevant algorithms to issue certificates:

sha256RSA withRSAEncryption	1.2.840.113549.1.1.11
SHA256 with ECDSA	1.2.840.10045.4.3.2

Subordinate CA certificates, subscriber certificates and OCSP certificates are not signed with sha-1WithRSAEncryption.

7.1.4. 名称形式 Name Forms

GDCA 签发的证书名称形式的格式和内容符合 X.501 Distinguished Name(DN)的甄别名格式。订户证书名称形式的格式和内容格式符合 RFC5280，及 CA/B 论坛发布的 TLS BRs 7.1.4 节的要求。

GDCA 根据本 CP/CPS 的要求签发证书，确保证书签发时，证书主题中的信息都是准确的。GDCA 不会将域名和 IP 地址写入证书主题属性中除非遵循本 CP/CPS 第 3.2.2.4 节和第 3.2.2.5 节的规定。

SSL/TLS 证书主题项不能仅含有诸如“.”，“-”，及“ ”（空格）字符，及/或其他任何表示该项为空、不完整、或不适用的内容。

The format and content of certificate names issued by GDCA comply with the Distinguished Name (DN) format defined in X.501. The format and content of subscriber certificate names comply with RFC 5280 and the requirements set forth in Section 7.1.4 of the CA/Browser Forum TLS BRs.

GDCA issues certificates in accordance with the requirements of this CP/CPS and ensures that the information contained in the certificate subject field is accurate at the time of issuance. GDCA shall not include domain names or IP addresses in certificate subject attributes unless such inclusion complies with the requirements set forth in Sections 3.2.2.4 and 3.2.2.5 of this CP/PS.

SSL/TLS server certificates cannot only contain metadata such as ‘.’, ‘-’ and ‘ ’ (empty) characters and/or any other indication that the value/field is absent, incomplete, or not applicable.

7.1.5. 名称限制 Name Constraints

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

GDCA may use the Name Constraints extension in accordance with RFC 5280 to restrict the scope of business applications for subordinate CA certificates.

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

证书策略对象标识符同本 CP/CPS 第 1.4.1.2 节。

See CP/CPS section1.4.1.2.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

7.2. 证书撤销列表 CRL Profile

GDCA 定期签发 CRL，供用户查询使用。

GDCA issues CRLs on a regular basis for inquiry and use by users.

7.2.1. 版本 Version Number(s)

GDCA 的证书撤销列表采用 X.509 v2 格式。

GDCA's Certificate Revocation Lists (CRLs) are issued in X.509 Version 2 format.

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

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

1. CRL 的版本号：用来指定 CRL 的版本信息，GDCA 采用的是同 X.509 V3 证书对应的 CRL V2 版本。
2. 签名算法：GDCA 采用 sha256RSA、sha256ECDSA、及 ECC 签名算法。
3. 颁发者：指定签发机构的 DN 名，由国家、省、市、机构、单位部门和通用名等组成。
4. 生效时间：指定一个日期/时间值，用以表明本 CRL 发布的时间。
5. 更新时间：指定一个日期/时间值，用以表明下一次 CRL 将要发布的时间（本标准强制使用该域）。
6. 撤销证书列表：指定已经撤销的证书列表。本列表中含有证书的序列号和证书被撤销的日期和时间。
7. 颁发机构密钥标识符（Issuer Unique Identifier）：本项标识用来验证在 CRL 上签名的公开密钥。它能辨别同一 CA 使用的不同密钥。
8. 理由码：若设置该项，则该 CRL 条目扩展项不得为关键扩展项。若 CRL 条目是针对根 CA 或中级 CA 证书的，则必须设置该 CRL 条目扩展项。若 CRL 条目是针对 SSL/TLS 订户证书，则 CRLReason 值不可为 certificateHold (6)。 若设置了 reasonCode 扩展项，则 CRLReason 值必须为 RFC5280 中最相关的理由。

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

1. CRL version: It refers to version information of CRL, GDCA adopts CRL V2 corresponding to X.509 V3 certificate.
2. Signature algorithm: GDCA adopts sha256RSA, sha256ECDSA and ECC signature algorithms.
3. Issuer: It refers to DN of issuing authority, including country, province, city, organization, department and common name, etc.
4. Effective time: It refers to date/time which indicates CRL issuing time.
5. Update time: It refers to date/time which indicates next issuing time of CRL. (It's an enforced field in this CP/CPS).
6. Certificate Revocation List: It refers to a list of revokedcertificates. The list contains certificate

serial number and certificate revocation date and time.

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

8. Reason Code: If present, this CRL entry extension shall not be marked critical. If a CRL entry is for a Root CA or subordinate CA certificate, this CRL entry extension shall be present. If a CRL entry is for a SSL/TLS certificate, the CRLReason shall not be certificateHold (6). If a reasonCode CRL entry extension is present, the CRLReason shall indicate the most appropriate reason for revocation of the certificate based on RFC 5280.

7.3. 在线证书状态协议 OCSP Profile

GDCA 采用 IETF PKIX 工作组开发的在线证书状态协议 (Online Certificate Status Protocol，OCSP，RFC6960)，该协议定义了一种标准的请求和响应信息格式以确认证书是否被撤销了。

若 OCSP 响应服务是为根证书或中级 CA 证书提供，且该类证书已被撤销，则在 CertStatus 的 RevokedInfo 中，revocationReason 字段必须设置。

CRLReason 必须为本 CP/CPS 第 7.2.2 章中允许的理由码。

GDCA adopts the Online Certificate Status Protocol (OCSP, RFC 6960) developed by the IETF PKIX Working Group. The protocol defines a standard request and response message format for determining whether a certificate has been revoked.

Where the OCSP response service is provided for a root certificate or a subordinate CA Certificate and such certificate has been revoked, the revocationReason field in the RevokedInfo structure of CertStatus shall be present.

The CRLReason indicated shall contain a value permitted for CRLs, as specified in section 7.2.2 of this CP/CPS.

7.3.1. 版本号 Version Number(s)

RFC6960 定义的 OCSP 版本。

The OCSP version defined in RFC 6960.

7.3.2. OCSP 扩展项 OCSP Extensions

不适用。OCSP 响应的 singleExtension 不可包含 CRL 条目的 reasonCode 扩展项。

Not Applicable. The singleExtension of an OCSP response cannot contain the reasonCode CRL entry extension.

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

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

GDCA 每季度内部进行一次一致性审计和运营评估，并每次抽取至少 3%数量的证书进行评估，以保证证书服务的可靠性、安全性和可控性。

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

1、GDCA 聘请独立的审计师事务所，按照 WebTrust 对 CA 的审计规则，每年进行一次外部审计和评估。

2、GDCA 每年进行一次风险评估工作，识别内部与外部的威胁，评估威胁事件发生的可能性及造成的损害，并评估目前的应对策略、技术、系统以及相关措施是否足够应对风险，根据风险评估，创建、实施并维持涵盖安全流程、措施及产品的安全计划。

GDCA conducts internal compliance audits and operational assessments on a quarterly basis and evaluates at least 3% of issued certificates during each assessment cycle in order to ensure the reliability, security, and controllability of its certificate services.

In addition to internal audits and assessments, GDCA engages independent auditing firms to conduct external audits and assessments in accordance with the WebTrust for CA criteria:

1. GDCA engages independent auditing firms to conduct external audits and assessments annually in accordance with the WebTrust for CA audit requirements.
2. GDCA performs annual risk assessments to identify internal and external threats, evaluate the likelihood and potential impact of threat events, and assess whether existing response strategies, technologies, systems, and related measures are sufficient to address such risks. Based on the results of the risk assessment, GDCA establishes, implements, and maintains a security program covering security processes, controls, and products.

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

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

GDCA 聘请的外部审计机构，应该具备以下的资质：

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

4. 具备独立审计的精神。

GDCA's internal audits are organized by the GDCA Security Policy Committee, which establishes a cross-department audit and assessment team to perform such activities.

External audit firms engaged by GDCA shall possess the following qualifications:

1. They shall be licensed and professionally qualified assessment institutions with a good reputation within the industry;
2. They shall possess knowledge of computer information security systems, communication network security requirements, PKI technologies, standards, and operations;
3. They shall possess the professional expertise and tools necessary to evaluate system operational performance;
4. They shall maintain independence and objectivity in conducting audits.

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

GDCA 审计员与本机构的系统管理员、业务管理员、业务操作员的工作岗位不能重叠。外部评估者和 GDCA 之间是独立的关系，双方无任何足以影响评估客观性的利害关系。

The roles of GDCA auditors shall not overlap with those of system administrators, business administrators, or business operators within the organization. External assessors shall maintain an independent relationship with GDCA, and neither party shall have any interest or relationship that could compromise the objectivity of the assessment.

8.4. 评估内容 Topics Covered by Assessments

GDCA 的审计工作包括以下内容：

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

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

The audit activities conducted within GDCA include, but are not limited to, the following:

1. Whether security policies have been adequately implemented;
2. Whether operational procedures and management policies are being strictly followed;

3. Whether certification services are performed in strict accordance with this CP/CPS, business specifications, and security requirements;
4. Whether various logs and records are complete and whether any anomalies exist;
5. Whether there are any other potential security risks.

Independent audits of GDCA are conducted by third-party auditing firms in accordance with the requirements of the WebTrust for CA criteria.

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

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

第三方审计师事务所评估完成后，GDCA 按照其工作报告进行整改，并接受再次审计和评估。

For issues identified in internal audit, the audit and assessment team shall be responsible for supervising the relevant departments in implementing improvements and corrective actions. Upon completion of the remediation activities, each department shall submit a summary report on the improvement efforts to the audit and assessment team.

Following completion of assessments conducted by third-party audit firms, GDCA shall perform remediation in accordance with the audit reports and shall undergo follow-up audits and assessments as required.

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

GDCA 的审计结果向本机构相关部门进行通报，对可能造成订户安全隐患，GDCA 将及时向订户通报。

第三方审计师事务所评估完成后，对于审计的结果，将通过 GDCA 官网进行公布。

GDCA communicates audit results to relevant internal departments. Where identified issues may pose security risks to subscribers, GDCA shall timely notify the affected subscribers.

Upon completion of assessments conducted by third-party audit firms, the audit results shall be published on the official GDCA website.

8.7. 自评估 Self-Audits

见 8.1 章节。

See section 8.1.

9. 法律责任和其他业务条款 Other Business and Legal Matters

9.1. 费用 Fees

9.1.1. 证书签发和更新 Certificate Issuance and Renewal Fees

GDCA 可根据提供的电子认证相关服务向本机构的证书订户收取费用，具体费用将取决于市场规则和相关管理部门的规定。GDCA 有权根据市场状况，针对不同订户群体推出不同的收费策略或优惠措施。

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

GDCA may charge fees to certificate subscribers for the certification services it provides. Specific fees shall be determined based on market practices and the requirements of relevant regulatory authorities. GDCA reserves the right to introduce different pricing strategies or preferential measures for different categories of subscribers in accordance with market conditions.

Where the pricing specified in an agreement executed by GDCA differs from the pricing publicly announced by GDCA, the pricing set forth in the agreement shall prevail.

9.1.2. 证书查询费用 Certificate Access Fees

在证书有效期内，对该证书信息进行查询，目前 GDCA 不收取查询费用。除非用户提出的特殊需求，需要 GDCA 支付额外的费用，GDCA 将与用户协商收取应该收取的费用。

如果证书查询的收费政策有任何变化，GDCA 将会及时在网站上予以公布。

During the validity period of a certificate, GDCA currently does not charge any fees for certificate information inquiry services. However, where a subscriber requests special services that require GDCA to incur additional costs, GDCA may charge appropriate fees subject to mutual agreement with the subscriber.

If there are any changes to the fee policy for certificate inquiry services, GDCA shall timely publish such changes on its website.

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

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

如果撤销和状态信息查询的收费政策有任何变化，GDCA 将会及时在网站上予以

公布。

GDCA currently does not charge any fees for certificate revocation or certificate status inquiry services. However, where a subscriber requests special services that require GDCA to incur additional costs, GDCA may charge appropriate fees subject to mutual agreement with the subscriber.

If there are any changes to the fee policy for revocation or certificate status inquiry services, GDCA shall promptly publish such changes on the official GDCA website.

9.1.4. 其他服务费用 Fees for Other Services

若 GDCA 将向用户提供证书存储介质及相关服务，GDCA 将在与订户或者其他实体签署的协议中指明该项价格。

Where GDCA provides certificate storage media and related services to subscribers, the applicable fees shall be specified in the agreements executed between GDCA and the subscribers or other relevant entities.

9.1.5. 退款策略 Refund Policy

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

在实施证书操作和签发证书的过程中，GDCA 遵守严格的操作程序和策略。如果 GDCA 违背了本 CP/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。

Except where certificate application or renewal fees may be refunded for specific reasons, GDCA generally does not refund any fees paid by subscribers.

In performing certificate operations and issuing certificates, GDCA complies with strict operational procedures and policies. If GDCA breaches the responsibilities or other material obligations set forth in this CP/CPS, the subscriber may request revocation of the certificate and a refund. Upon revocation of the subscriber's certificate, GDCA shall promptly refund in full the fees paid by the subscriber for the certificate application.

This refund policy does not limit the subscriber's right to seek other forms of compensation.

9.2. 财务责任 Financial Responsibility

9.2.1. 保险范围 Insurance Coverage

GDCA 按照 CA/B 论坛相关要求，投保了商业一般责任保险及专业责任保险

GDCA maintains Commercial General Liability insurance and Professional Liability/Errors and Omissions in accordance with the relevant requirements of the CA/Browser Forum.

9.2.2. 其他资产 Other Assets

不适用。

Not Applicable.

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

GDCA 如违反了本 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。

If GDCA fails to fulfill the obligations specified in this CP/CPS, certificate subscribers, relying parties, and other relevant entities may claim compensation from GDCA, except where liability is excluded by applicable laws or contractual agreements. Upon verification by GDCA, compensation may be provided to the affected entity. The limitations on compensation are as follows:

1. GDCA's total compensation liability shall not exceed the scope of insurance coverage specified in Section 9.2.1, and the amount of compensation shall not exceed the applicable liability limit. GDCA reserves the right to adjust the liability limit as appropriate and shall promptly notify the relevant parties of any such adjustment.
2. GDCA shall only assume liability for losses incurred during the validity period of the certificate.

9.3. 业务信息保密 Confidentiality of Business Information

9.3.1. 保密信息范围 Scope of Confidential Information

在 GDCA 提供的电子认证服务中，以下信息视为保密信息：

1) 审计记录包括：本地日志、服务器日志、归档日志的信息，这些信息被 GDCA 视为保密信息，只有安全审计员和业务管理员可以查看。除法律要求，不可在公司外部发布。

2) 其他由 GDCA 保存的个人和公司信息应视为保密，除法律要求，不可公布。

During the certification services provided by GDCA, the following information shall be regarded as confidential information:

1. Audit records, including local logs, server logs, and archived log information, shall be treated as confidential information by GDCA. Such information may only be accessed by security auditors and business administrators and shall not be disclosed outside the company unless required by law.
2. Other personal and corporate information retained by GDCA shall be treated as confidential and shall not be disclosed unless required by law.

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

GDCA 将以下信息视为不保密信息：

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

GDCA regards the following information as non-confidential information:

- Information contained in certificates and CRLs issued by GDCA;
- Information contained in certificate policies supported by GDCA and identified within the CP/CPS;
- Information authorized by GDCA for use by GDCA subscribers and publicly disclosed on the GDCA website;
- Other information whose confidentiality status depends on the specific data elements involved and the nature of the relevant application.

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

GDCA 有妥善保管与保护本节 9.3.1 中规定的保密信息的责任与义务。

GDCA has the responsibility and obligation to properly safeguard and protect the confidential information specified in Section 9.3.1.

9.4. 个人隐私保密 Privacy of Personal Information

9.4.1. 隐私保密方案 Privacy Plan

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

GDCA respects the privacy rights of certificate subscribers with respect to their personal information and fully complies with applicable laws, regulations, and national requirements relating to the protection of personal data privacy. At the same time, GDCA ensures that all personnel strictly adhere to applicable security and confidentiality standards in protecting personal privacy. Relevant policies concerning personal privacy protection may be accessed through the official GDCA website.

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

除了证书中已经包括的信息以及证书状态信息外，订户提供的其他基本信息将被视为隐私处理，GDCA 定义以下信息为证书订户的隐私信息：

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

Except for information already contained in certificates and certificate status information, other basic information provided by subscribers shall be treated as private information. GDCA defines the following information as subscriber private information:

- Subscribers' valid identification numbers, such as national identification card numbers and organizational code numbers;
- Subscribers' contact telephone numbers;
- Subscribers' mailing addresses and residential addresses;
- Subscribers' bank account information.

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

GDCA 定义包括但不限于以下信息不被视为证书订户的隐私信息：

- 订户姓名、单位名称等。
- 订户性别、单位性质等。
- 订户通信地址的邮政编码。

- 订户的电子邮箱。

GDCA defines the following information, including but not limited to, as not constituting subscriber private information:

- Subscriber names and organization names;
- Subscriber gender and organization type;
- Postal codes of subscriber mailing addresses;
- Subscriber email addresses.

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

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

GDCA has the responsibility and obligation to properly safeguard and protect the personal privacy information of certificate applicants specified in Section 9.4.2.

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

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

GDCA shall take appropriate measures to protect the personal privacy of certificate subscribers and shall employ reliable security measures to safeguard stored personal privacy information. Unless otherwise required by law or mandatory governmental regulations, GDCA shall not disclose any personal information of certificate subscribers, other than information included in digital certificates, to unrelated third parties (including organizations or individuals) without the prior consent of the certificate subscribers.

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

依据法律、行政法规、规章、决定、命令等，由于司法执行或法律授权的行政执行需要，GDCA 有可能需要将有关信息提供有关执法机关、行政执行机关。

Pursuant to applicable laws, administrative regulations, rules, decisions, orders, or other legal requirements, GDCA may be required to provide relevant information to judicial authorities or legally authorized administrative enforcement authorities for purposes of judicial enforcement or administrative enforcement.

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

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

Where a certificate subscriber requests specific customer support services from GDCA, such as document delivery services, GDCA may need to provide the subscriber's name, mailing address, and related information to third parties, such as courier or postal service providers.

9.5. 知识产权 Intellectual Property Rights

- GDCA 享有并保留对证书以及 GDCA 提供的所有软件的全部知识产权。
- GDCA 对数字证书系统软件具有所有权、名称权、利益分享权。
- GDCA 有权决定采用何种软件系统。
- GDCA 网站上公布的一切信息均为 GDCA 财产，未经 GDCA 书面允许，他人不能转载用于商业行为。
- GDCA 发行的证书和 CRL 均为受 GDCA 支配的财产。
- 对外运营管理策略和规范为 GDCA 财产。
- 用来表示目录中 GDCA 域中的实体的甄别名（以下简称 DN）以及该域中颁发给终端实体的证书，均为 GDCA 的财产。

- GDCA owns and retains all intellectual property rights in the certificates and all software provided by GDCA.
- GDCA holds ownership, naming rights, and benefit-sharing rights over the digital certificate system software.
- GDCA has the right to determine the software systems to be adopted.
- All information published on the GDCA website is the property of GDCA and may not be reproduced or used for commercial purposes without GDCA's prior written consent.
- Certificates and CRLs issued by GDCA are assets under the control of GDCA.
- External operational management policies and specifications are the property of GDCA.
- Distinguished Names (DNs) used to identify entities within the GDCA domain in directories, as well as certificates issued to end entities within that domain, are the property of GDCA.

9.6. 陈述与担保 Representations and Warranties

9.6.1. 电子认证服务机构的陈述与担保 CA Representations and Warranties

GDCA 在提供电子认证服务活动过程中的承诺如下：

- 签发给订户的证书符合 GDCA 的 CP/CPS 的所有实质性要求。
- 将向证书订户通报任何已知的，将在本质上影响订户的证书的有效性和可靠性事件。
- 将根据 CP/CPS 的要求及时撤销证书。
- 拒绝签发证书后，将立即向证书申请者归还所付的全部费用。
- 验证申请者对列在证书主题字段及主题别名扩展（或，仅针对域名而言，获得了拥有域名使用权或控制权人士的授权）中的域名及 IP 地址拥有使用权或控制权；
- 验证申请者授权了证书的签发以及申请者代表获得了授权，以代表申请者申请证书；
- 验证证书中所包含的全部信息的准确性；
- 根据 CP/CPS 3.2 的要求验证申请人的身份；
- 若 GDCA 与订户无关联，则 GDCA 与订户是合法有效且可执行的订户协议双方，该订户协议符合 CA/浏览器论坛发布的 TLS BRs 等要求；若 GDCA 与订户为同一实体或有关联，则申请人代表已认可使用条款；
- 针对所有未过期的证书的当前状态信息（有效或已撤销）建立及维护全天候的（24x7）公开的信息库。

证书公开发布后，GDCA 确保证书中的信息是经过验证的。

GDCA makes the following commitments in the course of providing certification services:

- Certificates issued to subscribers comply with all material requirements of GDCA's CP/CPS.
- GDCA will notify certificate subscribers of any known events that materially affect the validity or reliability of the certificates.
- GDCA will revoke certificates in a timely manner in accordance with the requirements of this CP/CPS.
- If a certificate request is rejected, GDCA will promptly refund all fees paid by the certificate applicant.
- GDCA verifies that the applicant has ownership or control rights over the domain names and IP addresses listed in the certificate subject field and subject alternative name extension (or, for domain names only, that authorization has been obtained from the party that owns or controls the domain name).
- GDCA verifies that the applicant has authorized the issuance of the certificate and that any authorized representative has been duly empowered to apply for the certificate on behalf of the applicant.

- GDCA verifies the accuracy of all information contained in the certificate.
- GDCA verifies the identity of applicants in accordance with Section 3.2 of the CP/CPS.
- That, if GDCA and subscribers are not affiliated, the subscriber and GDCA are parties to a legally valid and enforceable subscriber agreement that satisfies the TLS BRs and other requirements published by the CA/Browser Forum, or, if GDCA and subscribers are the same entity or are affiliated, the applicant representative acknowledged the terms of use.
- GDCA establishes and maintains a 24x7 publicly accessible repository of current status information (valid or revoked) for all unexpired certificates.

After a certificate is publicly issued, GDCA ensures that the information contained in the certificate has been verified.

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

GDCA 的注册机构在参与电子认证服务过程中的承诺如下：

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

GDCA Registration Authorities make the following commitments in the course of participating in electronic certification services:

1. The registration process provided to certificate subscribers fully complies with all material requirements of GDCA's CP/CPS.
2. When GDCA issues certificates, no discrepancy shall arise between the information in the certificate and the information of the certificate applicant due to errors made by the Registration Authority.
3. Registration Authorities shall submit revocation, renewal, and other service requests to GDCA in a timely manner in accordance with the CP/CPS.

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

订户一旦接受 GDCA 签发的证书，就被视为向 GDCA 及信赖证书的有关当事人作出以下承诺：

- 已知悉和接受 GDCA 的“订户协议”和本 CP/CPS 中的所有条款和条件。
- 订户在申请证书时向 GDCA 提供的信息都是真实、完整和准确的，愿意承担任何提供虚假、伪造等信息的法律责任。如果存在代理人，那么订户和代理人两者负有连带责任。订户有责任就代理人所作的任何不实陈述与遗漏，通知 GDCA。

- 订户须在安装及使用证书前，检查及核实证书内所载信息的准确性。
- 一经接受证书，即表示订户知悉和接受本 CP/CPS 中的所有条款和条件，并知悉和接受相应的订户协议。
- 一经接受证书，订户就应当承当如下责任：始终保持对其私钥的控制，使用可信的系统，采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用。
- 不得拒绝任何来自 GDCA 公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。
- 证书在本 CP/CPS 中规定使用范围内合法使用，只将证书用于经过授权的或其他合法的使用目的。
- 采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件。
- 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。
- 发现有任何实际或疑似滥用或泄露私钥的情况，应立即要求撤销该证书，并停止使用该证书及其相关的私钥。
- 如果证书中的任何信息已经或变得不正确或不准确，则立即要求撤销证书并停止使用证书。
- 在因密钥泄露的原因而撤销证书时，应立即停止使用证书中包含的与公钥对应的私钥。

Once a subscriber accepts a certificate issued by GDCA, the subscriber shall be deemed to have made the following commitments to GDCA and to all parties relying on the certificate:

- The subscriber has acknowledged and accepted all terms and conditions set forth in GDCA's Subscriber Agreement and this CP/CPS.
- All information provided by the subscriber to GDCA during the certificate application process is true, complete, and accurate. The subscriber agrees to bear any legal liability arising from the provision of false, forged, or misleading information. Where an agent is involved, both the subscriber and the agent shall bear joint and several liability. The subscriber is responsible for notifying GDCA of any false statements or omissions made by the agent.
- Subscribers shall examine and verify the accuracy of the information contained in the certificate before installing and using the certificate.
- Acceptance of the certificate constitutes acknowledgment and acceptance of all terms and conditions contained in this CP/CPS and the applicable Subscriber Agreement.
- Upon acceptance of the certificate, the subscriber assumes responsibility for maintaining continuous control over its private key, using trustworthy systems, and taking reasonable precautions to prevent loss, disclosure, tampering, or unauthorized use of the private key.

- The subscriber shall not reject or oppose any public notices, modifications, updates, or upgrades issued by GDCA, including but not limited to amendments to policies and specifications, or additions to or reductions in certificate services.
- The certificate shall be used lawfully within the scope specified in this CP/CPS and only for authorized or otherwise lawful purposes.
- The subscriber shall take secure and reasonable measures to prevent loss, disclosure, tampering, or compromise of the certificate private key.
- The subscribers undertake an obligation and warranty to install the certificates only on servers that are accessible at the subjectAltName(s) listed in the certificates.
- Immediately request revocation of the certificate and cease using the certificate and the associated private key upon becoming aware of any actual or suspected compromise, misuse, or unauthorized disclosure of the private key.
- Immediately request revocation of the certificate and cease using the certificate if any information contained in the certificate is, or becomes, incorrect or inaccurate.
- Where a certificate is revoked due to private key compromise, subscribers shall immediately cease using the private key corresponding to the public key contained in the certificate.

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

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

- Comply with all provisions of this CP/CPS.
- Confirm that certificates are used only within the permitted scope and validity period.
- Validate the certificate trust chain prior to relying on a certificate.
- Prior to relying on a certificate, confirm through CRL or OCSP queries whether the certificate has been revoked.
- Where, due to negligence or other reasons, a relying party fails to fulfill the obligations of reasonable verification, the relying party agrees to compensate GDCA for any resulting losses and to bear any losses incurred by itself or other parties as a consequence thereof.
- Not reject or oppose any public notices, modifications, updates, or upgrades issued by GDCA,

including but not limited to amendments to policies and specifications, or additions to or reductions in certificate services.

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

GDCA 从事电子认证活动的其他参与者作出如下承诺：遵守本 CP/CPS 的所有规定。

Other participants involved in GDCA's electronic certification activities make the following commitment: To comply with all provisions of this CP/CPS.

9.7. 担保免责 Disclaimers of Warranties

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

- 不保证证书订户、信赖方、其他参与者的陈述内容。
- 不对电子认证活动中使用的任何软件做出保证。
- 不对证书在超出规定目的以外的应用承担任何责任。
- 对由于不可抗力，如战争、自然灾害等造成的服务中断并由此造成的客户损失承担责任。
- 订户违反本 CP/CPS 9.6.3 之承诺时，或依赖方违反本 CP/CPS 9.6.4 之承诺时，得以免除 GDCA 之责任。

Except for the express commitments set forth in Section 9.6.1 of this CP/CPS, GDCA assumes no other warranties or obligations of any kind:

- GDCA does not warrant any representations made by certificate subscribers, relying parties, or other participants.
- GDCA makes no warranties regarding any software used in electronic certification activities.
- GDCA assumes no liability for the use of certificates beyond their intended purposes.
- GDCA shall not be liable for service interruptions or customer losses caused by force majeure events, including but not limited to war or natural disasters.
- GDCA shall be exempt from liability where subscribers breach the commitments set forth in Section 9.6.3 of this CP/CPS or where relying parties breach the commitments set forth in Section 9.6.4 of this CP/CPS.

9.8. 有限责任 Limitations of Liability

证书订户、依赖方因 GDCA 提供的电子认证服务从事民事活动遭受损失，GDCA 将承担不超过本 CP/CPS 9.9 规定的有限赔偿责任。

Where certificate subscribers or relying parties suffer losses in the course of engaging in civil

activities through the use of electronic certification services provided by GDCA, GDCA shall bear limited liability for compensation not exceeding the limits specified in Section 9.9 of this CP/CPS.

9.9. 赔偿 Indemnities

9.9.1. GDCA 的赔偿责任 Indemnification by GDCA

如 GDCA 违反了本 CP/CPS 9.6.1 中的陈述，证书订户、依赖方等实体可以申请 GDCA 承担赔偿责任（法定或约定免责除外）。如出现下述情形，GDCA 承担有限赔偿责任：

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

另外，GDCA 赔偿限制如下：

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

Where GDCA breaches the representations set forth in Section 9.6.1 of this CP/CPS, certificate subscribers, relying parties, and other relevant entities may seek compensation from GDCA, except where liability is excluded by applicable law or contractual agreement. GDCA shall bear limited liability under the following circumstances:

1. GDCA incorrectly issues a certificate to a third party other than the subscriber, resulting in losses to the subscriber or relying parties;
2. Where the information or documentation submitted by the subscriber is accurate and authentic, but the certificate issued by GDCA contains incorrect information, resulting in losses to the subscriber or relying parties;

3. GDCA knowingly issues a certificate despite being aware that the subscriber has submitted false or misleading information or documentation, resulting in losses to relying parties;
4. Due to reasons attributable to GDCA, a certificate private key is compromised, stolen, disclosed, or otherwise exposed, resulting in losses to the subscriber or relying parties;
5. GDCA fails to revoke a certificate in a timely manner, resulting in losses to relying parties.

In addition, GDCA's liability shall be subject to the following limitations:

1. GDCA's total liability for compensation shall not exceed the limits specified in Section 9.2.1 of this CP/CPS. Such liability limits may be revised by GDCA as appropriate.
2. GDCA's aggregate liability to any certificate subscriber, relying party, or other relevant entity relating to a certificate shall not exceed ten times the purchase price of the certificate.
3. GDCA shall not be liable for losses caused by the acts or omissions of subscribers or relying parties, and such losses shall be borne by the subscribers or relying parties themselves.
4. GDCA shall only assume liability for losses incurred during the validity period of the certificate.

9.9.2. 订户的赔偿责任 Indemnification by Subscribers

如因下述情形而导致 GDCA 或依赖方遭受损失，订户应当承担赔偿责任：

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

11. 在规定的范围外使用证书，如从事违法犯罪活动。

Where GDCA or relying parties suffer losses due to any of the following circumstances, the subscriber shall bear liability for compensation:

1. When applying for certificate registration, the subscriber intentionally, negligently, or maliciously provides false information or documentation, thereby causing damage to GDCA, its authorized certificate service agencies, or third parties;
2. The subscriber intentionally or negligently causes the disclosure or loss of its private key, fails to notify GDCA and its authorized certificate service agencies despite knowing that the private key has been disclosed or lost, or improperly delivers the private key to others for use, thereby causing damage to GDCA, its authorized certificate service agencies, or third parties;
3. The subscriber uses the certificate in violation of this CP/CPS or related operational specifications, or uses the certificate outside the scope of business permitted under this CP/CPS;
4. After a certificate subscriber or another authorized entity submits a certificate revocation request and before GDCA publishes the revocation information for the certificate, if the certificate is used for unlawful transactions or transaction disputes arise, the certificate subscriber shall bear all liability for damages, provided that GDCA has performed the relevant operations in accordance with this CP/CPS;
5. The information or documentation provided is false, incomplete, or inaccurate;
6. Information contained in the certificate changes, but the subscriber continues using the certificate without promptly notifying GDCA and relying parties;
7. The subscriber fails to take effective measures to protect the private key, resulting in loss, compromise, theft, or disclosure of the private key;
8. Upon becoming aware that the private key has been lost or compromised, the subscriber fails to discontinue use of the certificate and promptly notify GDCA and relying parties;
9. The subscriber continues to use the certificate after its expiration;
10. Information contained in the subscriber's certificate infringes the intellectual property rights of a third party;
11. The certificate is used outside the permitted scope, including for unlawful or criminal activities.

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

如因下述情形而导致 GDCA 或订户遭受损失，依赖方应当承担赔偿责任：

1. 没有履行 GDCA 与依赖方的协议和本 CP/CPS 中规定的义务；
2. 未能依照本 CP/CPS 规范进行合理审核，导致 GDCA 及其授权的证书服务机构或第三方遭受损害；
3. 在不合理的情形下信赖证书，如依赖方明知证书存在超范围、超期限使用的情

形或证书已经或有可能被人窃取的情形，但仍然信赖证书；

4. 依赖方没有对证书的信任链进行验证；
5. 依赖方没有通过查询 CRL 或 OCSP 确认证书是否被撤销。

Where GDCA or subscribers suffer losses due to any of the following circumstances, the relying party shall bear liability for compensation:

1. Failure to fulfill the obligations set forth in the agreement between GDCA and the relying party, or in this CP/CPS;
2. Failure to conduct reasonable verification in accordance with this CP/CPS, thereby causing damage to GDCA, its authorized certificate service agencies, or third parties;
3. Reliance on a certificate under unreasonable circumstances, such as where the relying party is aware that the certificate is being used beyond its permitted scope or validity period, or that the certificate has been or may have been compromised, but nevertheless continues to rely on the certificate;
4. Failure to validate the certificate trust chain;
5. Failure to confirm through CRL or OCSP queries whether the certificate has been revoked.

9.10.有效期限与终止 Term and Termination

9.10.1.有效期限 Term

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

This CP/CPS shall become effective at 00:00 on the date of publication, at which time the previous version of the CP/CPS shall simultaneously cease to be effective. This CP/CPS shall remain effective until the effective date of the next version of the CP/CPS or until GDCA terminates its electronic certification services.

9.10.2.终止 Termination

在 GDCA 终止电子认证服务时，本 CP/CPS 终止。

This CP/CPS shall terminate upon the termination of GDCA's certification services.

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

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

Upon termination of this CP/CPS, its validity shall simultaneously cease, and the provisions contained herein shall no longer apply. However, with respect to legal facts and events occurring

prior to the termination date, the provisions of this CP/CPS relating to the responsibilities and limitations of liability of the parties shall continue to apply.

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

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

Upon termination of this CP/CPS, GDCA shall notify all relevant parties participating in its certification activities regarding the invalidation of this document.

9.12. 修订 Amendments

9.12.1. 修订程序 Procedures for Amendment

经 GDCA 安全策略委员会授权，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。

Authorized by the GDCA Security Policy Committee, the CP/CPS Drafting Team shall review this CP/CPS at least once annually to ensure compliance with applicable national laws and regulations, requirements of competent authorities, relevant international standards, and the practical needs of certification business operations.

Any modification or update to this CP/CPS shall be proposed by the CP/CPS Drafting Team in the form of a revision report. Upon approval by the GDCA Security Policy Committee, the CP/CPS Drafting Team shall organize and implement the revision. The revised CP/CPS shall be formally published after receiving final approval from the GDCA Security Policy Committee.

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

修订后的 CP/CPS 经批准后将立即在 GDCA 的网站上发布。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。

The revised CP/CPS shall be published on the GDCA website immediately upon approval. For amendments requiring notification by email, written correspondence, media announcement, or other means, GDCA shall notify the relevant parties within a reasonable period of time. Such

reasonable period shall be sufficient to minimize the impact on the affected parties.

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

GDCA 负责确定 CP/CPS 的修订是否需要修改 OID。

GDCA shall be responsible for determining whether revisions to the CP/CPS require corresponding modifications to the OID.

9.13. 争议处理 Dispute Resolution Provisions

GDCA、证书订户、依赖方等实体在电子认证活动中产生争议可按以下步骤解决：

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

Any disputes arising among GDCA, certificate subscribers, relying parties, or other entities in connection with certification activities may be resolved in accordance with the following procedures:

1. Determine the responsible party in accordance with the provisions of this CP/CPS;
2. The relevant departments of GDCA shall coordinate with the applicant to seek resolution;
3. If such coordination fails, the dispute shall be resolved by the competent legal authorities;
4. Any litigation arising between GDCA and any party in relation to matters covered by this CP/CPS shall be subject to the jurisdiction of the People's Court at the place of GDCA's business registration.

9.14. 管辖法律 Governing Law

GDCA 的 CP/CPS 受中华人民共和国法律法规的管辖。

GDCA's CP/CPS shall be governed by the laws and regulations of the People's Republic of China.

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

无论 GDCA 的证书订户、依赖方等实体在何地居住以及在何处使用 GDCA 的证书，本 CP/CPS 的执行、解释和程序有效性均适用中华人民共和国的法律。任何与 GDCA 就本 CP/CPS 所涉及的任何争议，均适应中华人民共和国法律。

Regardless of where GDCA certificate subscribers, relying parties, or other entities reside or where GDCA certificates are used, the execution, interpretation, and procedural validity of this CP/CPS

shall be governed by the laws of the People's Republic of China. Any disputes relating to this CP/CPS involving GDCA shall also be governed by the laws of the People's Republic of China.

9.16. 一般条款 Miscellaneous Provisions

9.16.1. 完整协议 Entire Agreement

GDCA 的 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。

The complete document structure of GDCA's CP/CPS consists of three parts: the title, the table of contents, and the main body. Any revised replacement content relating to the table of contents or the main body shall fully supersede all previous corresponding sections and shall be published on the GDCA website for reference and review.

9.16.2. 转让 Assignment

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。此转让行为发生时不影响到转让方对另一方的任何债务及责任的更新。

GDCA declares that, in accordance with the rights and obligations of the parties to the certification activities as detailed in this CP/CPS, the parties may transfer their respective rights and obligations in accordance with applicable laws and regulations. Such transfer shall not affect or release the transferring party from any debts, liabilities, or responsibilities owed to the other parties.

9.16.3. 分割性 Severability

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

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

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

If any provision of this CP/CPS, or its application, is held to be invalid or unenforceable due to a

conflict with the laws of the jurisdiction in which GDCA operates, GDCA may amend such provision to the minimum extent necessary to ensure its continued validity and enforceability, while the remaining provisions shall remain unaffected. GDCA shall disclose the details of such amendments in this section.

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

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

9.16.4.强制执行（律师费用和权利放弃）Enforcement (Attorneys' Fees and Waiver of Rights)

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

GDCA declares that a failure by certificate subscribers, relying parties, or other entities to comply with any provision of GDCA's CP/CPS shall not be construed as a waiver of the obligation to comply with such provision or any other provision in the future.

9.16.5.不可抗力 Force Majeure

GDCA 不对因战争、瘟疫、火灾、地震和其他天灾等不可抗力的事件所造成本 CP/CPS 规定担保责任的违反、延误或无法履行负责。

GDCA shall not be liable for any breach, delay, or failure in the performance of the warranties or obligations set forth in this CP/CPS caused by force majeure events, including but not limited to war, epidemics, fire, earthquakes, or other natural disasters.

9.17. 其他条款 Other Provisions

GDCA 对本 CP/CPS 具有最终解释权。

GDCA reserves the final right of interpretation of this CP/CPS.