数安时代科技股份有限公司

EV 证书电子认证业务规则

Global Digital Cybersecurity Authority CO., LTD.

EV Certificate Certification Practice Statement

(EV CPS)

Version: V1.7

Release Date:April 25, 2018

Effective Date:May 1, 2018

目录

Contents

1. 引言 Introduction 1
   1.1. 概述 Overview 1
      1.1.1. 公司简介 Company Profile 1
      1.1.2. 电子认证业务规则（CPS）Certification Practice Statement (CPS) 2
   1.2. GDCA 架构 GDCA Certificate Hierarchical Architecture 3
      1.2.1. GDCA EV 证书层次架构 GDCA EV Certificate Hierarchical Architecture 5
   1.3. 文档名称与标识 Document Name and Identification 8
   1.4. 电子认证活动参与者 PKI Participants 9
      1.4.1. 电子认证服务机构 Certification Authorities 9
      1.4.2. 注册机构 Registration Authorities 9
      1.4.3. 订户 Subscribers 9
      1.4.4. 依赖方 Relying Parties 10
      1.4.5. 其他参与者 Other Participants 10
   1.5. 证书应用 Certificate Usage 10
      1.5.1. 适合的证书应用 Appropriate Certificate Uses 10
      1.5.2. 限制的证书应用 Prohibited Certificate Uses 11
   1.6. 策略管理 Policy Administration 12
      1.6.1. 策略文档管理机构 Organization Administering the Document 12
      1.6.2. 联系人 Contact Person 12
      1.6.3. 决定 CPS 符合策略的机构 Person Determining CPS Suitability for the Policy 13
      1.6.4. CPS 批准程序 CPS Approval Procedures 13
      1.6.5. CPS 修订 CPS Revision 13
   1.7. 定义和缩写 Definitions and Acronyms 14
      1.7.1. 术语定义一览表 List of Term Definition 14
      1.7.2. 缩略语及其含义一览表 List of Abbreviations and their Meaning 17
2. 信息发布与信息管理 Publication and Repository Responsibilities 17
   2.1. GDCA 信息库 Repositories 17
   2.2. 信息的发布 Publication of Information 18
   2.3. 发布的时间和频率 Time or Frequency of Publication 18
   2.4. 信息库访问控制 Access Controls on Repositories 19
3. 身份标识与鉴别 Identification and Authentication 19
   3.1. 命名 Naming 19
      3.1.1. 名称类型 Type of Names 19
      3.1.2. 对名称意义化的要求 Need for Names to be Meaningful 22
      3.1.3. 订户的匿名或伪名 Anonymity or Pseudonymity of Subscribers 23
      3.1.4. 理解不同名称的形式的规则 Rules for Interpreting Various Name Forms 23
      3.1.5. 名称的唯一性 Uniqueness of Names 23

3.1.6. 商标的识别、鉴别与角色 Recognition, Authentication, and Role of Trademarks 23
3.2. 初始身份确认 Initial Identity Validation 24
3.2.1. 证明拥有私钥的方法 Method to Prove Possession of Private Key 24
3.2.2. 机构身份的鉴别 Authentication of Organization Identity 24
3.2.3. 个人身份的鉴别 Authentication of Individual Identity 28
3.2.4. 没有验证的订户信息 Non-Verified Subscriber Information 28
3.2.5. 授权确认 Validation of Authority 28
3.2.6. 互操作准则 Criteria for Interoperation 29
3.2.7. 数据来源的准确性 Data Source Accuracy 29
3.3. 密钥更新请求的标识与鉴别 Identification and Authentication for Rekey Requests 30
3.3.1. 常规密钥的更新的标识与鉴别 Identification and Authentication for Routine Rekey 30
3.3.2. 吊销后密钥更新的标识与鉴别 Identification and Authentication for Rekey After Revocation 31
3.4. 吊销请求的标识与鉴别 Identification and Authentication for Revocation Request 31
3.5. 授权服务机构的标识和鉴别 Identification and Authentication for Authorized Service Organization 31
4. 证书生命周期操作要求 Certificate Life Cycle Operational Requirements 31
4.1. 证书申请 Certificate Application 31
4.1.1. 证书申请实体 Who Can Submit a Certificate Application 31
4.1.2. 注册过程与责任 Enrollment Process and Responsibilities 32
4.2. 证书申请处理 Certificate Application Processing 32
4.2.1. 识别与鉴别功能 Performing Identification and Authentication Functions 32
4.2.2. 证书申请批准和拒绝 Approval or Rejection of Certificate Applications 33
4.2.3. 处理证书申请的时间 Time to Process Certificate Applications 35
4.2.4. 认证机构授权（CAA） Certification Authority Authorization (CAA) . 35
4.3. 证书签发 Certificate Issuance 36
4.3.1. 电子认证服务机构（CA）的行为 CA Actions 36
4.3.2. CA 通知订户证书的签发 Notifications to Subscriber of Issuing the Certificate 37
4.4. 证书接受 Certificate Acceptance 37
4.4.1. 构成接受证书的行为 Conduct Constituting Certificate Acceptance 37
4.4.2. 电子认证服务机构对证书的发布 Publication of the Certificate by the CA 37
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 38
4.5. 密钥对和证书的使用 Key Pair and Certificate Usage 38
4.5.1. 订户的私钥和证书的使用 Subscriber Private Key and Certificate Usage 38
4.5.2. 依赖方公钥和证书的使用 Relying Party Public Key and Certificate

Usage 39
4.6. 证书更新 Certificate Renewal 40
4.6.1. 证书更新的情形 Circumstances for Certificate Renewal 40
4.6.2. 请求证书更新的实体 Who May Request Renewal 40
4.6.3. 证书更新请求的处理 Processing Certificate Renewal Requests 40
4.6.4. 颁发新证书时对订户的通告 Notification of New Certificate Issuance to Subscriber 40
4.6.5. 构成接受更新证书的行为 Conduct Constituting Acceptance of a Renewal Certificate 40
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 40
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 41
4.7. 证书密钥更新 Certificate Rekey 41
4.7.1. 证书密钥更新的情形 Circumstances for Certificate Rekey 41
4.7.2. 请求证书密钥更新的实体 Who May Request Certification of a New Public Key 41
4.7.3. 证书密钥更新请求的处理 Processing Certificate Rekeying Requests ... 41
4.7.4. 颁发新证书时对订户的通告 Notification of New Certificate Issuance to Subscriber 42
4.7.5. 构成接受密钥更新证书的行为 Conduct Constituting Acceptance of a Rekeyed Certificate 42
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 42
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 42
4.8. 证书变更 Certificate Modification 42
4.8.1. 证书变更的情形 Circumstances for Certificate Modification 43
4.8.2. 请求证书变更的实体 Who May Request Certificate Modification 43
4.8.3. 证书变更请求的处理 Processing Certificate Modification Requests 43
4.8.4. 颁发新证书时对订户的通告 Notification of New Certificate Issuance to Subscriber 43
4.8.5. 构成接受变更证书的行为 Conduct Constituting Acceptance of Modified Certificate 43
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 43
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 44
4.9. 证书吊销和挂起 Certificate Revocation and Suspension 44
4.9.1. 证书吊销的情形 Circumstances for Revocation 44
4.9.2. 请求证书吊销的实体 Who Can Request Revocation 47
4.9.3. 吊销请求的流程 Procedure for Revocation Request 48
4.9.4. 问题和报告处理机制 Processing Mechanism of Problems and Reports 49
4.9.5. 吊销请求宽限期 Revocation Request Grace Period 50

4.9.6. 电子认证服务机构处理吊销请求的时限 Time Within Which CA Must Process the Revocation Request 51
4.9.7. 依赖方检查证书吊销的要求 Revocation Checking Requirements for Relying Parties 51
4.9.8. CRL 发布频率 CRL Issuance Frequency 51
4.9.9. CRL 发布的最大滞后时间 Maximum Latency for CRLs 51
4.9.10. 在线状态查询的可用性 Online Revocation/Status Checking Availability 52
4.9.11. 在线状态查询要求 Online Revocation Checking Requirements 52
4.9.12. 吊销信息的其他发布形式 Other Forms of Revocation Advertisements Available 52
4.9.13. 密钥损害的特别要求 Special Requirements related to Key Compromise 53
4.9.14. 证书挂起的情形 Circumstances for Suspension 53
4.9.15. 请求证书挂起的实体 Who Can Request Suspension 53
4.9.16. 挂起请求的流程 Procedure for Suspension Request 53
4.9.17. 挂起的期限限制 Limits on Suspension Period 53
4.10. 证书状态服务 Certificate Status Services 54
4.10.1. 操作特征 Operational Characteristics 54
4.10.2. 服务可用性 Service Availability 54
4.10.3. 可选特征 Operational Features 54
4.11. 订购结束 End of Subscription 55
4.12. 密钥托管与恢复 Key Escrow and Recovery 55
4.12.1. 密钥托管与恢复的策略与行为 Key Escrow and Recovery Policy and Practices55
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 55
5. 认证机构设施、管理和操作控制 Facility, Management, and Operational Controls 56
5.1. 物理控制 Physical Controls 56
5.1.1. 场地位置与建筑 Site Location and Construction 56
5.1.2. 物理访问 Physical Access 58
5.1.3. 安防监控 Security Monitoring 59
5.1.4. 电力与空调 Power and Air Conditioning 60
5.1.5. 水患防治 Water Exposures 60
5.1.6. 火灾防护 Fire Prevention and Protection 61
5.1.7. 介质存储 Media Storage 62
5.1.8. 废物处理 Waste Disposal 62
5.1.9. 异地备份 Off-Site Backup 62
5.2. 程序控制 Procedural Controls 62
5.2.1. 可信角色 Trusted Roles 62
5.2.2. 每项任务需要的角色 Number of Persons Required per Task 63
5.2.3. 每个角色的识别与鉴别 Identification and Authentication for Each Role 63
5.2.4. 需要职责分割的角色 Roles Requiring Separation of Duties 63

5.3. 人员控制 Personnel Controls 64
5.3.1. 资格、经历和无过失要求 Qualifications, Experience, and Clearance Requirements 64
5.3.2. 背景审查程序 Background Check Procedures 65
5.3.3. 培训要求 Training Requirements 67
5.3.4. 再培训周期和要求 Retraining Frequency and Requirements 68
5.3.5. 工作岗位轮换周期和顺序 Job Rotation Frequency and Sequence 68
5.3.6. 未授权行为的处罚 Sanctions for Unauthorized Actions 68
5.3.7. 独立合约人的要求 Independent Contractor Requirements 68
5.3.8. 提供员工的文档 Documentation Supplied to Personnel 69
5.4. 审计日志程序 Audit Logging Procedures 70
5.4.1. 记录事件的类型 Types of Events Recorded 70
5.4.2. 处理日志的周期 Frequency of Processing Log 71
5.4.3. 审计日志的保存期限 Retention Period for Audit Log 72
5.4.4. 审计日志的保护 Protection of Audit Log 72
5.4.5. 审计日志备份程序 Audit Log Backup Procedures 72
5.4.6. 审计收集系统 Audit Collection System (Internal vs. External) 72
5.4.7. 对导致事件实体的通告 Notification to Event-Causing Subject 73
5.4.8. 脆弱性评估 Vulnerability Assessments 74
5.5. 记录归档 Records Archival 74
5.5.1. 归档记录的类型 Types of Records Archived 74
5.5.2. 归档记录的保存期限 Retention Period for Archive 75
5.5.3. 归档文件的保护 Protection of Archive 75
5.5.4. 归档文件的备份程序 Archive Backup Procedures 75
5.5.5. 记录时间戳要求 Requirements for Time-Stamping of Records 76
5.5.6. 归档收集系统 Archive Collection System (Internal or External) 76
5.5.7. 获得和检验归档信息的程序 Procedures to Obtain and Verify Archive Information 76
5.6. 电子认证服务机构密钥的更替 Key Changeover 77
5.7. 损害与灾难恢复 Compromise and Disaster Recovery 78
5.7.1. 事故和损害处理程序 Incident and Compromise Handling Procedures .. 78
5.7.2. 计算资源、软件和或/数据的损坏 Computing Resources, Software, and/or Data Are Corrupted 78
5.7.3. 实体私钥损害处理程序 Entity Private Key Compromise Procedures 79
5.7.4. 灾难后的业务连续性能力 Business Continuity Capabilities After a Disaster 81
5.8. 电子认证服务机构或注册机构的终止 CA or RA Termination 82
5.9. 数据安全 Data Security 83
6. 认证系统技术安全控制 Technical Security Controls 83
6.1. 密钥对的生成与安装 Key Pair Generation and Installation 83
6.1.1. 密钥对的生成 Key Pair Generation 83
6.1.2. 私钥传送给订户 Private Key Delivery to Subscriber 84
6.1.3. 公钥传送给证书签发机构 Public Key Delivery to Certificate Issuer 84
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. 密码算法技术标准 Key Sizes 85
6.1.6. 公钥参数的生成和质量检查 Public Key Parameters Generation and Quality Checking 85
6.1.7. 密钥使用目的 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 88
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 Method of Activating Private Key 88
6.2.9. 解除私钥激活状态的方法 Method of Deactivating Private Key 89
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 Capabilities 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 90
6.4. 激活数据 Activation Data 91
6.4.1. 激活数据的产生和安装 Activation Data Generation and Installation 91
6.4.2. 激活数据的保护 Activation Data Protection 92
6.4.3. 激活数据的其他方面 Other Aspects of Activation Data 93
6.5. 计算机安全控制 Computer Security Controls 94
6.5.1. 特别的计算机安全技术要求 Specific Computer Security Technical Requirements 94
6.5.2. 计算机安全评估 Computer Security Rating 95
6.6. 生命周期技术控制 Life Cycle Technical Controls 95
6.6.1. 系统开发控制 System Development Controls 95
6.6.2. 安全管理控制 Security Management Controls 96
6.6.3. 生命周期的安全控制 Life Cycle Security Controls 97
6.7. 网络的安全控制 Network Security Controls 97
6.8. 时间戳 Time-Stamping 98
7. 证书、证书吊销列表和在线证书状态协议 Certificate, CRL, and OCSP Profiles 98
7.1. 证书 Certificate Profile 98
7.1.1. 版本 Version Number(s) 99
7.1.2. 证书扩展项 Certificate Extensions 99
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 103
7.1.6. 证书策略对象标识符 Certificate Policy Object Identifier 103
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语义 Processing Semantics for the Critical Certificate Policies Extension 104
7.2. 证书吊销列表 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 104
7.3. 在线证书状态协议 OCSP Profile 105
7.3.1. 版本号 Version Number(s) 106
7.3.2. OCSP 扩展项 OCSP Extensions 106
7.3.3. OCSP 请求和响应处理 Processing of OCSP Request and Response ... 107
8. 认证机构审计和其他评估 Compliance Audit and Other Assessments 108
8.1. 评估的频率或情形 Frequency and Circumstances of Assessment 108
8.2. 评估者的资质 Identity/Qualifications of Assessor 110
8.3. 评估者与被评估者之间的关系 Assessor's Relationship to Assessed Entity 110
8.4. 评估内容 Topics Covered by Assessment 111
8.5. 对问题与不足采取的措施 Actions Taken as a Result of Deficiency 111
8.6. 评估结果的传达与发布 Communications of Results 112
9. 法律责任和其他业务条款 Other Business and Legal Matters 112
9.1. 费用 Fees 112
9.1.1. 证书签发和更新 Certificate Issuance or Renewal Fees 112
9.1.2. 证书查询费用 Certificate Access Fees 113
9.1.3. 证书吊销或状态信息的查询费用 Revocation or Status Information Access Fees 113
9.1.4. 其他服务费用 Fees for Other Services 114
9.1.5. 退款策略 Refund Policy 114
9.2. 财务责任 Financial Responsibility 115
9.2.1. 保险范围 Insurance Coverage 115
9.2.2. 其他财产 Other Assets 116
9.2.3. 对最终实体的保险或担保 Insurance or Warranty Coverage for End-Entities 116
9.2.4. 责任免除 Liability Exemption 116
9.3. 业务信息保密 Confidentiality of Business Information 119
9.3.1. 保密信息范围 Scope of Confidential Information 119
9.3.2. 不属于保密的信息 Information Not Within the Scope of Confidential Information 119
9.3.3. 保护保密信息的责任 Responsibility to Protect Confidential Information 120
9.4. 个人隐私保密 Privacy of Personal Information 120
9.4.1. 隐私保密方案 Privacy Plan 120
9.4.2. 作为隐私处理的信息 Information Treated as Private 120
9.4.3. 不被视为隐私的信息 Information Not Deemed Private 121

9.4.4. 保护隐私的责任 Responsibility to Protect Private Information 121
9.4.5. 使用隐私信息的告知与同意 Notice and Consent to Use Private Information 121
9.4.6. 依法律或行政程序的信息披露 Disclosure Pursuant to Judicial or Administrative Process 122
9.4.7. 其他信息披露情形 Other Information Disclosure Circumstances 122
9.5. 知识产权 Intellectual Property Rights 122
9.6. 陈述与担保 Representations and Warranties 123
9.6.1. 电子认证服务机构的陈述与担保 CA Representations and Warranties 123
9.6.2. 注册机构的陈述与担保 RA Representations and Warranties 125
9.6.3. 订户的陈述与担保 Subscriber Representations and Warranties 125
9.6.4. 依赖方的陈述与担保 Relying Party Representations and Warranties .. 127
9.6.5. 其他参与者的陈述与担保 Representations and Warranties of Other Participants 128
9.7. 担保免责 Disclaimers of Warranties 128
9.8. 有限责任 Limitations of Liability 129
9.9. 赔偿 Indemnities 129
9.9.1. GDCA 的赔偿责任 Indemnification by GDCA 129
9.9.2. 订户的赔偿责任 Indemnification by Subscribers 130
9.9.3. 依赖方的赔偿责任 Indemnification by Relying Parties 132
9.10. 有效期限与终止 Term and Termination 132
9.10.1. 有效期限 Term 132
9.10.2. 终止 Termination 133
9.10.3. 效力的终止与保留 Effect of Termination and Survival 133
9.11. 对参与者的个别通告与沟通 Individual Notices and Communications with Participants 133
9.12. 修订 Amendments 133
9.12.1. 修订程序 Procedure for Amendment 133
9.12.2. 通知机制和期限 Notification Mechanism and Period 134
9.12.3. 必须修改业务规则的情形 Circumstances Under Which CPS Must be Changed 134
9.12.4. 对象标识符变更 Object Identifier Modification 134
9.13. 争议处理 Dispute Resolution Provisions 134
9.14. 管辖法律 Governing Law 135
9.15. 与适用法律的符合性 Compliance with Applicable Law 135
9.16. 一般条款 Miscellaneous Provisions 135
9.16.1. 完整协议 Entire Agreement 135
9.16.2. 转让 Assignment 136
9.16.3. 分割性 Severability 136
9.16.4. 强制执行 Enforcement 137
9.16.5. 不可抗力 Force Majeure 137
9.17. 其他条款 Other Provisions 137
附录 1：证书信息 Appendix 1: Certificate information 138
附录 2：GDCA EV 证书电子认证业务规则修订记录表 Appendix 2: GDCA EV CPS

Revision Records..... 140

1. 引言 Introduction

1.1. 概述 Overview

1.1.1. 公司简介 Company Profile

数安时代科技股份有限公司（Global Digital Cybersecurity Authority Co., Ltd.，简称 GDCA 或“数安时代”）原为“广东数字证书认证中心有限公司”，成立于 2003 年 3 月 6 日。2005 年 9 月，GDCA 依法通过了国家密码管理局和原国家信息产业部的资格审查，成为全国首批八家获得《电子认证服务许可证》（许可证号：ECP4401021007）的电子认证服务机构之一；2008 年 12 月，获得国家密码管理局颁发的《商用密码产品销售许可证》；2011 年 4 月，通过了国家密码管理局电子政务电子认证服务能力评估，获得《电子政务电子认证服务机构》（编号：A021）资格。2013 年，对电子认证服务系统进行 SM2 算法升级，并通过了国家密码管理局组织的安全性审查。2015 年，GDCA 通过了 WebTrust 国际安全审计认证，具备了国际标准化的运营管理和服务水平，可以提供全球化的电子认证服务。为适应业务发展需要，2016 年 5 月，“广东数字证书认证中心有限公司”更名为“数安时代科技股份有限公司”。2017 年 8 月 11 日，GDCA 开始在新三板挂牌交易，股票简称：数安时代，股票代码：871932。

Global Digital Cybersecurity Authority CO., LTD. (abbreviated as GDCA, or “数安时代”) with the former name of Guangdong Digital Certificate Authority CO., LTD was founded on March 6, 2003. In September 2005, GDCA passed the security review by the State Cryptography Administration Office of Security Commercial Code Administration (abbreviated as OSCCA) and the former Ministry of Information Industry by law, as one of the first eight electronic authentication authorities granted the "Electronic Authentication Service License" (license number: ECP4401021007) in China. In December 2008, GDCA obtained the "Commercial Cryptography Products Sales License" issued by OSCCA. GDCA passed through the assessment of E-government and Electronic Authentication Service Ability by OSCCA with the qualification certificate of "E-government and Electronic Authentication Service Authority" (number: A021) in April 2011. In 2013, GDCA upgraded electronic authentication service system for SM2 algorithm and passed through the security review by OSCCA. In 2015, GDCA passed the assurance review for Certification Authority by WebTrust with the international level of operation management and service to provide digital certification service globally. For business development, GDCA changed its name from "Guangdong Digital Certificate Authority CO., LTD." to "Global Digital Cybersecurity Authority CO., LTD." in May, 2016. On 11 August 2017, GDCA was admitted to the National Equities Exchange and Quotations (NEEQ) of China, with a stock abbreviation of “数安时代” and stock code “871932”.

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

本着“权威、创新、服务、公信”的运营理念，GDCA 致力于为电子商务、电子政务及社会信息化等应用提供优质的电子认证服务。

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

With a business philosophy of “Authority, Innovation, Services and Credibility”, GDCA has been and will continue to dedicate itself in offering electronic authentication services of high quality to industries including e-commerce, e-governance, and social informatization etc.

1.1.2. 电子认证业务规则（CPS）Certification Practice Statement (CPS)

本电子认证业务规则（简称 EV CPS）描述了 GDCA 签发 EV 证书时所遵循的程序，符合 CA/浏览器论坛（CA/Browser Forum，国际组织，又称国际 CA 浏览器联盟，是制定 CA 国际标准的机构，www.cabforum.org）发布的 Guidelines for the Issuance and Management of Extended Validation Certificates（简称“EV Guidelines”）以及 Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates （简称“EV Code Signing Guidelines”），即扩展验证证书指南（Guidelines for Extended Validation Certificates）的要求。

This Certification Practice Statement (abbreviated as EV CPS) describes the procedures which GDCA should follow for issuing EV certificate. It meets the requirements of Guidelines for the Issuance and Management of Extended Validation Certificates(hereinafter referred to as “EV Guidelines”), and Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates (hereinafter referred to as “EV Code Signing Guidelines”), namely the Guidelines for Extended Validation Certificates published by CA/Browser Forum (an organization, which is also called international CA browser alliance, lays down International Standard of CA) at www.cabforum.org.

本 CPS 适用于 GDCA 的 EV ROOT CA、EV SSL CA、EV CodeSigning CA，以及相关用户、订户、依赖方等实体。本 CPS 作为一个单独的文件，涵盖了签发和管理 EV 证书相关的具体操作和流程。

按照本 CPS 签发的 EV 证书，其对象是向 GDCA 申请并通过所有相关身份鉴别的各类机构。

所有 GDCA EV 证书的订户及依赖方必须参照本 CPS 及相应 CP 的规定，决定对证书的使用和信任。

This CPS applies to GDCA EV ROOT CA, EV SSL CA, EV CodeSigning CA, and related users, subscribers, relying parties, etc. This CPS is considered as an individual document, covering relevant specific operations and processes about the issuance and management of EV certificate.

GDCA issues certificates to the entitles which apply for an EV certificate and have pass all relevant identification according to this CPS.

All subscribers and relying parties of GDCA EV certificates must refer to the provisions of this CPS and the corresponding CP so as to decide the usage and trust for the certificates.

GDCA 遵循 WebTrust 国际标准（Trust Service Principles and Criteria for Certification Authorities）及 CA/浏览器论坛（CA/Browser Forum）发布的扩展验证证书指南的最新版本要求进行签发和管理 EV 数字证书，定期查看其更新情况，并将持续根据其发布的版本进行修订 CPS。如果本 CPS 和 CA/浏览器论坛（CA/Browser Forum）发布的相关规范中的条款有不一致的地方，则以 CA/浏览器论坛正式发布的规范为准。

GDCA issue and manage the EV certificates based on the latest version of Guidelines for the Issuance And Management of Extended Validation Certificates and Guidelines for the Issuance And Management of Extended Validation Code Signing Certificates published by Trust Service Principles and Criteria for Certification Authorities and CA/Browser Forum, GDCA regularly checks the status on CA/Browser Forum's website and continuously revise this CPS if there is any update. In the event that a discrepancy arises between interpretations of this document and CA/Browser Forum, the CA/Browser Forum shall govern.

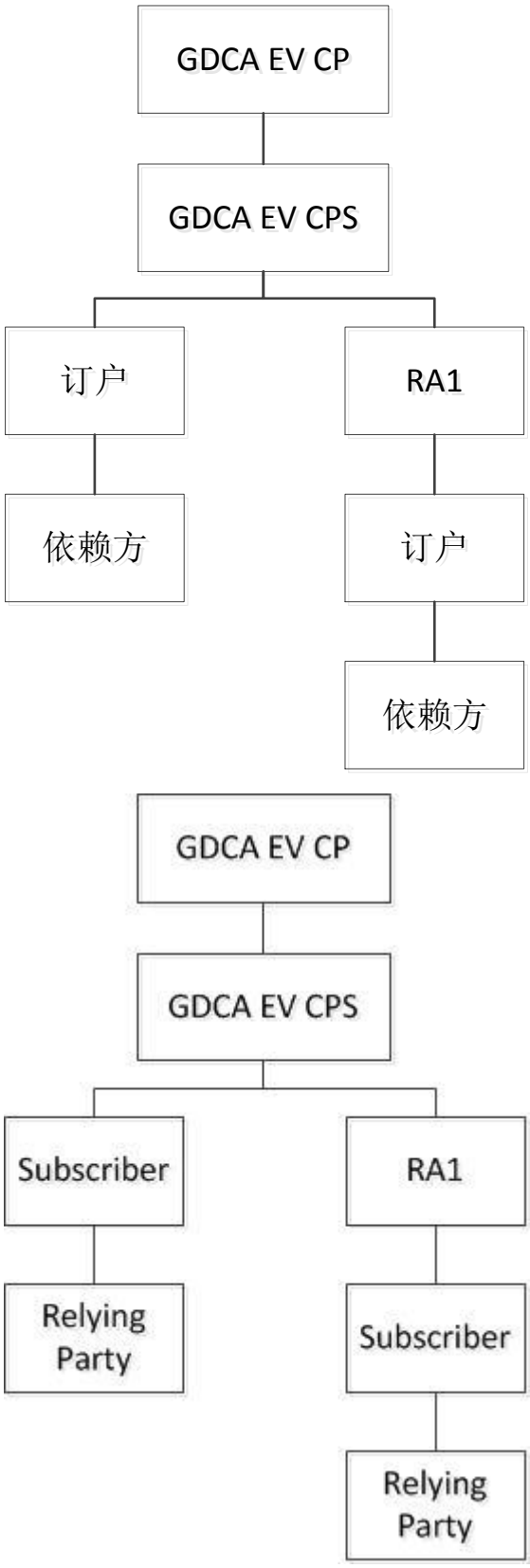
1.2. GDCA 架构 GDCA Certificate Hierarchical Architecture

本 CPS 按照 GDCA EV CP 制定，GDCA 按照本 CPS 进行证书服务申请鉴别，订户、依赖方及其他相关实体按照本 CPS 及 EV CP 决定对证书的使用、信任并履行相关的义务。

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

This CPS formulates follow the GDCA EV CP. GDCA carries out certificate service application identification according to this CPS. Subscribers, relying parties and other relevant entities decide the usage and trust of the certificate and perform the relevant obligations according to this CPS and EV CP.

This document is the Chinese-English bilingual edition of GDCA EV CPS. If there is any inconsistency or conflict between the Chinese and English versions, the Chinese version shall prevail for all purposes.

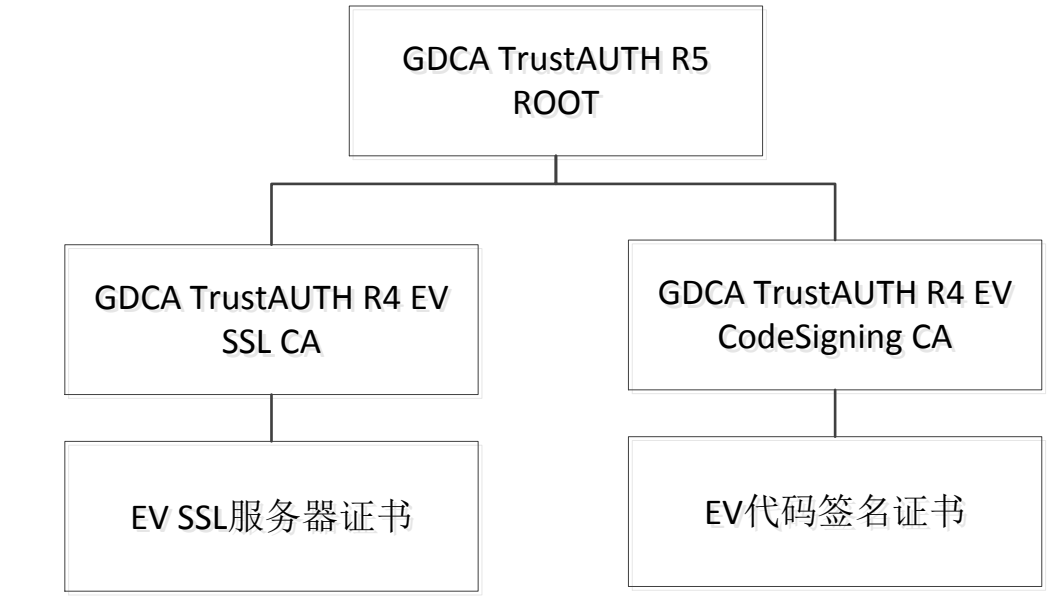

GDCA EV CP
GDCA EV CPS
订户
RA1
依赖方
订户
依赖方
GDCA EV CP
GDCA EV CPS
Subscriber
RA1
Relying Party
Subscriber
Relying Party

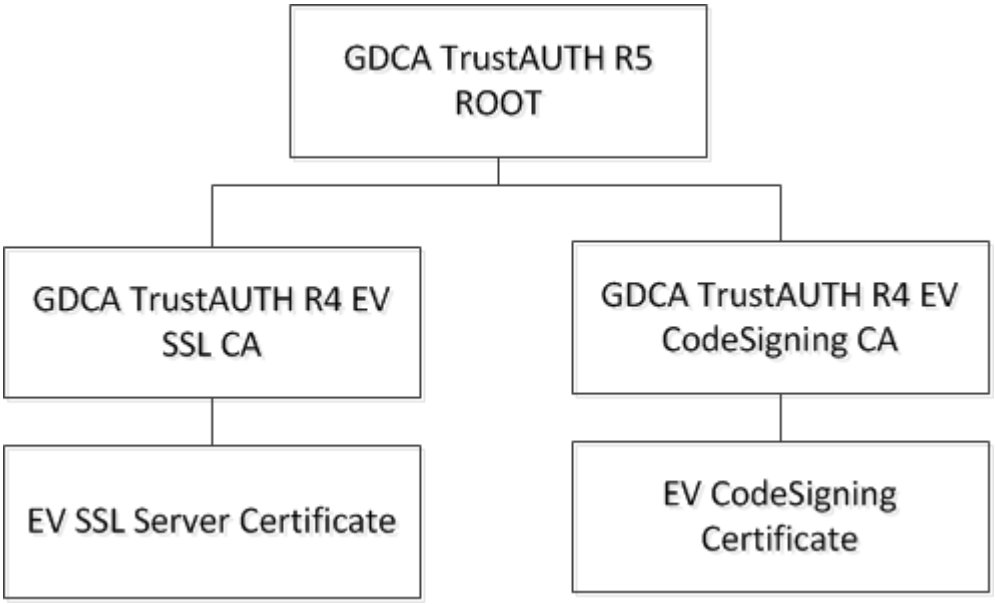
1.2.1. GDCA EV 证书层次架构 GDCA EV Certificate Hierarchical Architecture

GDCA 目前有 3 个 EV 根证书，分别为 GDCA TrustAUTH R5 ROOT 证书、数安时代 R5 根 CA 证书、GDCA TrustAUTH E5 ROOT 证书。每个根 CA 下设中级 CA，以签发用户证书。GDCA 不签发外部中级 CA 证书。

Currently, GDCA has 3 EV root certificates, including GDCA TrustAUTH R5 ROOT certificate, 数安时代 R5 根 CA certificate, GDCA TrustAUTH E5 ROOT certificate.

1) GDCA TrustAUTH R5 ROOT





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

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

GDCA TrustAUTH R5 ROOT 证书将于 2040 年 12 月 31 日到期。

GDCA TrustAUTH R4 EV SSL CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

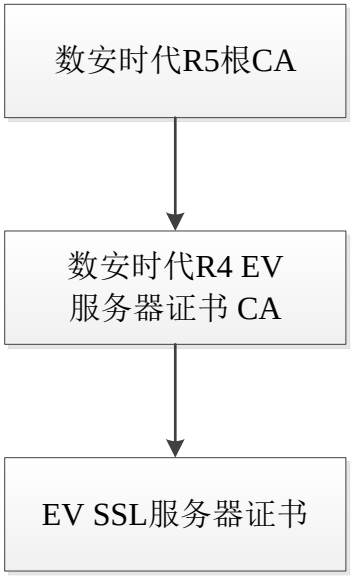
GDCA TrustAUTH R4 EV CodeSigning CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

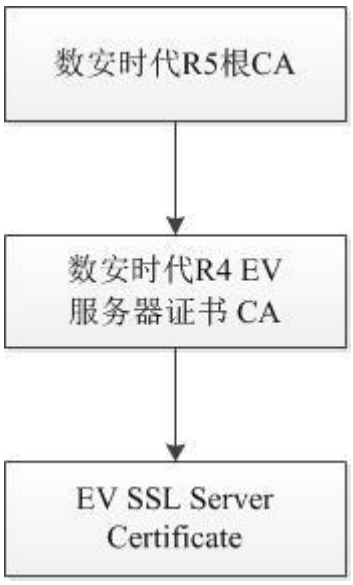
GDCA TrustAUTH R5 ROOT certificate will expire on December 31, 2040.

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

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

2) 数安时代 R5 根 CA





数安时代 R5 根 CA 证书的根密钥长度为 4096-bit，下设 1 个中级 CA 证书：数安时代 R4 EV 服务器证书 CA，密钥长度为 2048-bit，签发密钥长度为 2048-bit 的 EV SSL 服务器证书。

数安时代 R5 根 CA 证书将于 2040 年 12 月 31 日到期。

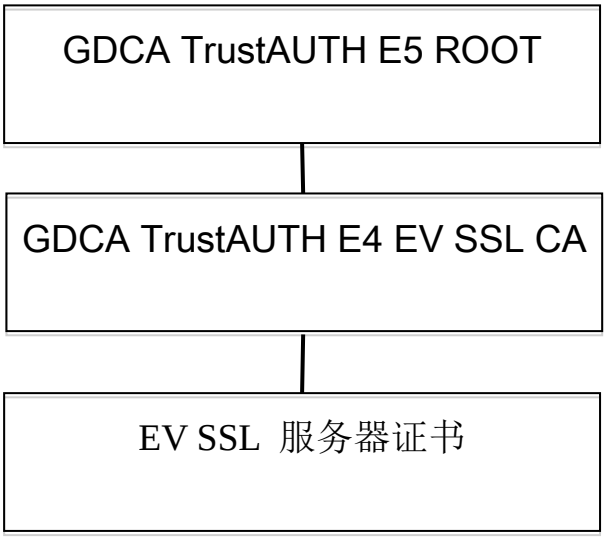
数安时代 R4 EV 服务器证书 CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

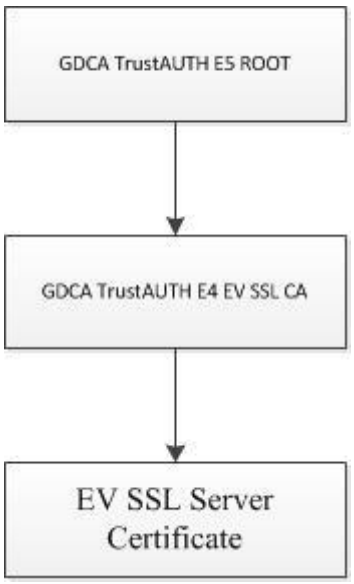
The length of 数安时代 R5 根 CA certificate root key is 4096-bit. There is one Subordinate CA under this ROOT CA, including: 数安时代 R4 EV 服务器证书 CA with 2048-bit key length is responsible for issuing 2048-bit EV SSL Server Certificates.

数安时代 R5 根 CA certificate will expire on December 31, 2040.

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

3) GDCA TrustAUTH E5 ROOT





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

GDCA TrustAUTH E5 ROOT 证书将于 2040 年 12 月 31 日到期。

GDCA TrustAUTH E4 EV SSL CA 证书将在 2030 年 12 月 31 日到期，2027 年 1 月 1 日起，将不再使用该 CA 证书签发订户证书。

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

GDCA TrustAUTH E5 ROOT certificate will expire on December 31, 2040.

GDCA TrustAUTH E4 EV SSL CA certificate will expire on December 31, 2030. From January 1, 2027, GDCA will no longer use it to issue subscriber certificates.

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

本文档称作《数安时代科技股份有限公司 EV 证书认证业务规则 V1.7 版》（简称《GDCA EV CPS V1.7》、本 CPS）。有关本版本 CPS 的修订信息请参考附录 2。

本 CPS 的对象标识符（OID）与《数安时代科技股份有限公司 EV 证书策略》（简称《GDCA EV CP》）中的对象标识符一致。

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

This document calls "Global Digital Cybersecurity Authority CO., LTD. EV Certificate Certification

Practice Statement V1.7"(abbreviated as “GDCA EV CPS” or “this CPS”). Please refer to Appendix 2 for detailed revisions of this version.

The object identifier (OID) of this CPS is consistent with "Global Digital Cybersecurity Authority CO., LTD. EV Certificate Policy” (abbreviated as “GDCA EV CP”).

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

1.4. 电子认证活动参与者 PKI Participants

1.4.1. 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，依法设立的第三方电子认证服务机构。GDCA 通过给从事电子交易活动的各方主体颁发 EV 数字证书、提供证书验证服务等手段而成为电子认证活动的参与主体。

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

1.4.2. 注册机构 Registration Authorities

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

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

Registration Authority (RA) establishes registration process, confirms the identities of EV certificate applicants, and approves or rejects the request of EV certificate applicants on behalf of CA.

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

1.4.3. 订户 Subscribers

在电子签名应用中，订户即是电子签名人、证书持有人，是 GDCA 颁发证书的所有最终用户。

本 CPS 中出现的订户，均指各类机构。GDCA 只对各类机构发放 EV 证书，不

向自然人提供 EV 证书服务。

In the application of electronic signature, subscribers also called electronic signers or certificate holders are end users of the certificates issued by GDCA.

Subscribers who appear in this CPS refer to various organizations. GDCA only issues EV certificate to various organizations, and don't provide EV certificate service to natural person.

1.4.4. 依赖方 Relying Parties

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

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

1.4.5. 其他参与者 Other Participants

其他参与者是指为 GDCA 的电子认证活动提供相关服务的其他实体。

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

1.5. 证书应用 Certificate Usage

1.5.1. 适合的证书应用 Appropriate Certificate Uses

GDCA 签发的 EV 证书主要用于身份识别。

依据本 CPS 签发的 EV SSL 证书，可用来验证证书中标识的域名的身份，以及持有该域名的法人机构身份；依据本 CPS 签发的 EV CodeSigning 证书，可用来验证证书中标识的软件代码提供方或发布方的身份。凡是经过验证后确定是由 GDCA 签发的 EV 证书，均表明该证书中所包含的信息真实有效，并且已经通过了适当且可靠的身份鉴别程序。

EV certificate issued by GDCA is mainly used for identification.

EV SSL certificate issued according to this CPS can be used to verify the identity of domain name indicated in certificate and the identities of legal authorities which hold the domain name above. EV CodeSigning certificates issued according to this CPS can be used to verify the identity of software code supplier or publisher indicated in the certificate. After verifying the issuer of EV certificate is GDCA, it shows that the information contained in the certificate is true and effective, and has

passed the appropriate and reliable authentication procedure.

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

EV SSL 服务器证书用于验证证书中标识的网络主机服务器或互联网域名的身份，以及持有该网络服务器或互联网域名的法人机构身份。GDCA 不签发通配符 EV SSL 服务器证书， EV SSL 服务器证书不限制域名的种类，如商业域名、政府域名等。

EV SSL server certificate is used for verifying the identity of server or domain name and organization who owns this server or domain name. GDCA does not issue wildcard EV SSL server certificate. The types of domain names in EV SSL server certificates are not restricted, e.g. .com, .gov etc.

1.5.1.2. EV 代码签名证书 EV CodeSigning Certificates

EV 代码签名证书用于验证证书中标识的软件代码提供方或发布方的身份。

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

1.5.2. 限制的证书应用 Prohibited Certificate Uses

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

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

In addition to the scope of the above provisions, GDCA EV certificate is not designed for, not intended for, not authorized for control equipment in danger, or for the occasion where the failure is required to avoid, such as operation of nuclear equipment, navigation or communication systems of shuttles, control systems of air traffic or weapons, since these faults or failures may lead to death, personal injury or serious environmental damage.

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

1.6. 策略管理 Policy Administration

GDCA 安全策略委员会是 GDCA 电子认证服务所有策略的最高管理机构，负责审核批准 CPS，并作为 CPS 实施检查监督的最高决定机构。

GDCA Security Policy Committee is the highest management authority responsible for review and approval of policies of electronic certification services, as well as the highest decision organization to perform inspection and supervision of the enforcement of CPS.

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

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

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

本策略文档的对外咨询服务等日常工作由行政管理部门负责。

GDCA Security Policy Committee is assigned as the document management authority responsible for establishing, publishing and updating this CPS. The committee consists of the relevant representatives with the right of decision-making from GDCA's management, administrative center, marketing center, technology center, operation and service center, etc.

Member of GDCA Security Policy Management Committee has the right to vote over management and approval of certificate policy. The Chairman of the committee may have two votes for decision in case of tie of votes.

Consultation of this policy document to the external parties and other routine jobs are undertaken by the administrative department.

1.6.2. 联系人 Contact Person

GDCA 将对电子认证业务规则进行严格的版本控制，并由 GDCA 指定专门的机构负责相关事宜。任何有关 CPS 的问题、建议、疑问等，都可以按以下方式进行联系。

联系部门：GDCA 行政管理部门

联系人：王女士

网站地址：https://www.gdca.com.cn/

电子邮箱地址：gdca@gdca.com.cn

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

邮政编码：510030

电话号码：020-83487228

传真号码：020-83486610

Specialized agencies who are designated by GDCA take the responsibility of strict version control of CPS. Any problems, suggestions, questions, etc., about this CPS, you could contact us as follows::

Contact Department: GDCA Administrative Department

Contact: Ms. Wang

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

E-mail: gdca@gdca.com.cn

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

Postal Code: 510030

Tel: 020-83487228

Fax: 020-83486610

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

GDCA 安全策略委员会是公司 CPS 策略制定的最高权威机构，审定批准 CPS，是决定 CPS 符合策略的机构。

As the highest organization for making CPS, GDCA Security Policy Committee is a decision-making organization to ensure the CPS is in line with CP which is responsible for examination and approval of the CPS.

1.6.4. CPS 批准程序 CPS Approval Procedures

本机构的 CPS 由 GDCA 安全策略委员会组织 CPS 编写小组拟定文档，CPS 编写小组完成后提交 GDCA 安全策略委员会审核批准。

This CPS is drafted by the team designated by GDCA Security Policy Committee. After the completion of drafting, the CPS is submitted to GDCA Security Policy Committee for review.

1.6.5. CPS 修订 CPS Revision

GDCA 根据国家的政策法规、技术要求、业务发展情况以及 CA/浏览器论坛

（CA/Browser Forum）发布的扩展验证证书指南（Guidelines for Extended Validation Certificates）的最新要求及时修订本 CPS，CPS 编写小组根据相关的情况拟定 CPS 修订建议，提交 GDCA 安全策略委员会审核，经该委员会批准后，正式在 GDCA 官方网站上发布。

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

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

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

1.7. 定义和缩写 Definitions and Acronyms

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

GDCA	数安时代科技股份有限公司的缩写
GDCA 安全策略委员会	GDCA 认证服务体系内的最高策略管理监督机构和 CPS 一致性决定机构
电子认证服务机构	GDCA 及授权的下级操作中级 CA 被称为电子认证服务机构（Certificate Authority，CA），也就是证书认证机构，是颁发证书的实体。
注册机构	注册机构（Registration Authority，RA）负责处理证书申请者和证书订户的服务请求，并将之提交给认证服务机构，为最终证书申请者建立注册过程的实体，负责对证书申请者进行身份标识和鉴别，发起或传递证书撤销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。
本地注册受理点	本地注册受理点（Local Registration Authority）是受理证书服务的终端机构，作为 GDCA 认证服务体系架构内直接面向用户的服务主体，经过 CA 或 RA 的授权从事各类服务。
录入员	负责录入证书申请者提交的信息，协助用户办理数字证书申

	请、撤销、更新等手续。
审核员	负责审核证书申请信息，协助用户办理数字证书申请、撤销、更新等手续。
电子签名认证证书	电子认证服务提供者签发的用以证明证书持有人的电子签名、身份、资格即其他有关信息的电子文件。
数字证书	使用数字签名作为识别签名人身份和表明签名人认可签名数据的一种电子签名认证证书。
电子签名	具有识别签名人身份和表明签名人认可签名数据的功能的技术手段。
数字签名	通过使用非对称密码加密系统对电子记录进行加密、解密变换来实现的一种电子签名。
电子签名人	是指持有电子签名制作数据并以本人身份或者以其所代表的名义实施电子签名的人。
电子签名依赖方	是指基于对电子签名认证证书或者电子签名的信赖而从事有关活动的人。
私钥（电子签名制作数据）	在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。
公钥（电子签名验证数据）	是指订户验证电子签名的数据。
订户	从电子认证服务机构接收证书的实体，也被称为证书持有人。在电子签名应用中，订户即为电子签名人。
依赖方	依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。

GDCA	Abbreviation for Global Digital Cybersecurity Authority CO., LTD.
GDCA Security Policy Committee	It is the highest management and monitor function for CPS and the decision-making agency pursuant to CPS within the GDCA certification services system.
The electronic certification service authority	GDCA and authorized subordinate CA are called as electronic certification service authority, also known as the certificate authority, and they are the entities to issue the certificate.
Registration Authority	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 electronic certification service authority.
Local Registration Authority	As the entity serves to users directly in GDCA authentication service system, LRA is the end authority providing certificate services authorized by CA or RA.
Entry Clerk	Entry clerk is responsible for inputting the information submitted by the applicant and help the user handle certificates application, revocation and renewal procedures etc.
Reviewer	The reviewer is responsible for checking the information of certificate application and help the user handle certificates application, revocation and renewal procedures etc.
Electronic Signature Certificate	Electronic Signature Certificate is issued by the electronic certification authority to prove the electronic signature, identity, qualification and other relevant electronic information of the certificate holder.
Digital certificate	Digital certificate is used as a digital signature certificate used for identifying authorization and indicating that the signer has recognized the signature.
Electronic signature	Electronic signature is a technical mean for identifying authorization and indicating that the signer has recognized the signature.
Digital signature	An electronic signature uses asymmetric encryption system for encrypting or decrypting electronic data.
Electronic signer	Electronic signer is a person who holds electronic signature data to generate data in his/her own name or to perform electronic sign-off on behalf of the person he represents.
the relying party on electronic signature	The relying party on electronic signature is the person who engages in the relevant activities based on his trust in the electronic certificate or electronic signature.
private key (creation data of electronic signature)	In the course of the use of electronic signatures, private key is the data such as character, encoding, etc. associate the reliably electronic signatures with the signer.
public key (validation data of electronic signature)	Public key refers to the subscriber's validation data of electronic signature.
Subscribers	Subscriber is the entity receiving the certificate from the electronic certification authority, known as certificate holders. In the applications of electronic signature, subscriber is an electronic signatory.

relying party	A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued by CA. A Relying party may, or may not be a Subscriber.

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

CA	Certificate Authority	电子认证服务机构
CP	Certification Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则
CRL	Certificate Revoke List	证书撤消列表
GDCA	Global Digital Cybersecurity Authority CO., LTD.	数安时代科技股份有限公司
KM	Key Management Center	密钥管理中心
LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
LRA	Local Registration Authority	本地注册受理点
OCSP	Online Certificate Status Protocol	在线证书状态协议
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	公共密钥基础设施
RA	Registration Authority	注册审核服务机构
RFC	Request For Comments	请求评注标准(一种互联网建议标准)

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

2.1. GDCA 信息库 Repositories

GDCA 信息库是一个对外公开的信息库，它能够保存、取回证书及与证书有关的信息。GDCA 信息库内容包括但不限于以下内容：CP 和 CPS 现行和历史版本、证书、CRL、订户协议，以及其它由 GDCA 不定期发布的信息。GDCA 将及时发布包括证书、CPS 修订和其它资料等内容，这些内容必须保持与 CPS 和有关法律法规一致。GDCA 信息

库可以通过网址：https://www.gdca.com.cn 查询，或由 GDCA 随时指定的其它通讯方法获得。

GDCA repositories are open to the public. It can store, retrieve certificates and their related information. GDCA repository includes but is not limited to the following: current and historical CPs and CPSs, certificates, CRLs, subscriber agreements and other information published irregularly by GDCA. GDCA will release certificates, CP and CPS revisions and so on timely that must remain consistent with the CPS, relevant laws and regulations. You can search at https://www.gdca.com.cn or via any other communication methods specified by GDCA at any time.

2.2. 信息的发布 Publication of Information

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

GDCA 通过目录服务器发布订户的证书和 CRL，订户或依赖方可以通过访问 GDCA 的目录服务器获取证书的信息和吊销证书列表；同时，GDCA 提供在线证书状态查询服务，订户或依赖方可实时查询证书的状态信息。

同时，GDCA 也将会根据需要采取其他可能的形式进行信息发布。

GDCA publishes repositories on its official website (https://www.gdca.com.cn). The official website is the primary, most prompt and authoritative channel to publish all information about GDCA.

GDCA publishes certificates and CRLs via LDAP. Subscriber or relying party can obtain information of certificates and CRLs through LDAP. Meanwhile, subscriber or relying party can check the current status of certificate instantly via OCSP service provided by GDCA.

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

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

GDCA 在订户证书签发或者注销时，通过目录服务器或官方网站自动将证书和 CRL 发布，发布周期为不大于 24 小时，即在 24 小时内发布最新 CRL；在紧急的情况下，GDCA 可以自行决定证书和 CRL 的发布时间。GDCA 每年发布一次电子认证服务机构的 CA 证书撤销列表（ARL）。

信息库其他内容的发布时间和频率，由 GDCA 独立做出决定，这种发布应该是即时的、高效的，并且是符合国家法律的要求的。

GDCA releases automatically the latest certificates and CRLs via LDAP or official website within 24 hours after the certificates are issued or revoked. In particular, GDCA can choose time to release the certificates and CRL in case of an emergency. GDCA releases CRL of CA (ARL) every year.

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

2.4. 信息库访问控制

Access Controls on Repositories

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

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

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

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

3. 身份标识与鉴别 Identification and Authentication

3.1. 命名 Naming

3.1.1. 名称类型 Type of Names

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

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

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

EV certificates issued by GDCA conform to X.509 standard and Distinguished Name of subject conforms to X.500 standard

Naming rules and requirements of EV SSL certificate and EV code signing certificate must be

stated in this CPS customized according to GDCA EV CP, and in line with Section 9 requirements of Guidelines published by CA/ browser Forum at www.cabforum.org. Distinguished Name of EV SSL certificate and EV CodeSigning certificate must contain common name (Common Name, CN=), which shall be validated and contains domain name, organization e-mail address, organization legal name, etc.

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

GDCA 证书颁发机构的主体甄别名命名规则如下：

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

Naming rules of issuer's DN in GDCA certificate are as follows:

Attribute	Value
Country（C）	CN
State（S）	State of issuer (if included)
Local（L）	Local of issuer (if included)
Organization（O）	Global Digital Cybersecurity Authority CO.,LTD. or GDCA Certificate Authority
Organization Unit（OU）	Certificate contains various issuers depend on subscriber types, applications and regions to issue the certificate.
Common Name（CN）	Name of CA

GDCA 证书订户的主体甄别名命名规则如下：

属性	值
国家（C）	CN
省（S）	订户所在省份，或者不用

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

Naming rules of Subject Distinguished Name in subscriber's certificate of GDCA are as follows:

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

EV Root 证书甄别名命名规则

属性	值
国家（C）	CN
机构（O）	GUANG DONG CERTIFICATE AUTHORITY CO., LTD.
通用名（CN）	GDCA TrustAUTH R5 ROOT

Naming rules of Distinguished Name in EV Root certificate are as follows:

Attribute	Value
Country（C）	CN
Organization（O）	GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.
Common Name	GDCA TrustAUTH R5 ROOT

（CN）	

EV SSL CA 证书甄别名命名规则

属性	值
国家（C）	CN
机构（O）	Global Digital Cybersecurity Authority Co., Ltd.
通用名（CN）	GDCA TrustAUTH R4 EV SSL CA

Naming rules of Distinguished Name in EV SSL CA certificate are as follows:

Attribute	Value
Country（C）	CN
Organization（O）	Global Digital Cybersecurity Authority Co., Ltd.
Common Name（CN）	GDCA TrustAUTH R4 EV SSL CA

EV CodeSigning CA 证书甄别名命名规则

属性	值
国家（C）	CN
机构（O）	Global Digital Cybersecurity Authority Co., Ltd.
通用名（CN）	GDCA TrustAUTH R4 EV CodeSigning CA

Naming rules of Distinguished Name in EV CodeSigning CA certificate are as follows:

Attribute	Value
Country（C）	CN
Organization（O）	Global Digital Cybersecurity Authority Co., Ltd.
Common Name（CN）	GDCA TrustAUTH R4 EV CodeSigning CA

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

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

Names in certificates should have a significant meaning. Subject name should definite the identities

of certificate holders and server, domain name or software publisher. This name should be identified by relying parties and meet the requirements of laws and regulations.

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

本 CPS 规定，GDCA 的订户在进行数字证书申请时不能使用匿名或伪名。

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

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

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

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

3.1.5. 名称的唯一性 Uniqueness of Names

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

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

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

GDCA 签发的证书的主体甄别名中不包含商标名。

Subject’s DN of certificate issued by GDCA does not contain any trademarks.

3.2. 初始身份确认 Initial Identity Validation

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

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

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

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

GDCA 仅向机构用户提供 EV 证书申请服务，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、机构合法成立的文件和复印件、业务办理授权书、主管人、经办人有效身份证件的原件和复印件以及其他证明文件。

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 发布的指南的要求。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。

GDCA only provides EV certificate application service to institutional subscribers. When applying for the EV certificate, it is required to submit digital certificate application form, original and copy of organization validity, authorization letter of operation, original and copy of institute supervisor, operator’s resident identity card, or other documents according to the types of certificate.

Authentication and review procedures of organization identity are in compliance with the requirements of guideline published by CA/ browser Forum at www.cabforum.org. At the same time, when there are internationalized domain names (IDNs) in the certificate application, GDCA will verify the identity of the domain name holder to detect whether there exists homographic spoofing behavior of IDNs.

3.2.2.1. 鉴别要求 Authentication requirements

EV 证书只面向政府机关、企业单位、事业单位、社会团体以及其他机构提供，对于申请人必须进行以下鉴别和验证：

1. 必须依法存在
2. 证书申请人和与合法注册的机构名称一致
3. 证书申请经办人必须获得机构授权

EV certificates are only provided to government agencies, enterprises, public institutions, social organizations and other institutions. The following identification and verification of the applicant will be conducted:

1. The legal identity of applicant is valid.
2. The name of the applicant is in accordance with the name of valid registration organization.
3. The representative of applicant must obtain the authorization from the institution.

3.2.2.2. 鉴别方法 Authentication methods

1. 机构身份确认
   (1) 验证组织机构代码证、工商营业执照（或营业执照）、社会团体登记证、事业单位登记证等相关证明文件
   (2) 通过查询第三方数据库等方式验证机构名称、注册信息等与申请人提交的信息是否一致
   (3) 验证机构经营地址或经营场所
   (4) 验证电话号码等机构联系方式

1. Organization identity confirmation

(1) Verify organization code certificate, business license (or normal license), social organization registration certificate, public institution registration certificate and other relevant proof documents.

(2) Verify the consistency of organization name, registration information and information submitted by applicant by cross-checking third-party database, etc.

(3) Verify institution's operation address or place.

(4) Verify phone number or other contacts info of institution.

2. 证书申请经办人身份确认
   (1) 验证经办人身份证、护照等个人身份证明材料
   (2) 验证银行卡、电话账单等证明材料
   (3) 验证经办人的授权办理证明文件
   (4) 通过电话、邮件等方式与机构人事部门联系，确认相关人员身份及授权

2. Certificate application handling person identity confirmation

(1) Confirming identity of representative of applicant, passport and other individual identity proof information.

(2) Verify bank card and telephone bill, etc.

(3) Verify handling authorized proof document of representative.

(4) Confirm the identity and authorization of relevant personnel from telephone or email, etc.

3. 域名确认

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

(1) 通过该域名注册服务机构或权威第三方数据库中查询到的该域名持有者登记的电子邮件或电话号码，以发送电子邮件或拨打电话的方式与域名持有者取得联系，询问申请材料中的关键信息内容（如：申请者的证件信息、域名信息等），确认其对域名的所有权。鉴别方式遵循 Baseline Requirments v1.5.6 第 3.2.2.4.3 节和第 3.2.2.4.4 节。

(2) 在包含 FQDN（完全限定域名）的 URI（统一资源标识符）的在线网页上对约定的信息进行改动，通过此方式以确认申请者对 FQDN 的实际控制权。鉴别方式遵循 Baseline Requirments v1.5.6 第 3.2.2.4.6 节。

(3) 通过确认申请域名在 DNS CNAME、TXT 或 CAA 记录中的任意值或请求令牌的存在来确认申请人对 FQDN（完全限定域名）的控制。鉴别方式遵循 Baseline Requirments v1.5.6 第 3.2.2.4.7 节。

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。

GDCA 不为 IP 地址签发 EV SSL 证书。

3. Domain validation

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:

- Obtain the e-mail address or phone number of the domain name owner listed by the domain name registrar or other authoritative third party database, and check the key information (e.g. documentation information or domain name details etc.) with the owner by emails or phone calls to confirm its ownership of the domain name. This way of validation conforms to section 3.2.2.4.3 and section 3.2.2.4.4 of the Baseline Requirements v1.5.6.
- By making a change to the agreed-upon information found on an online Web page identified by a uniform resource identifier containing the FQDN, to confirm the applicant's practical

control over the FQDN. This way of validation conforms to section 3.2.2.4.6 of the Baseline Requirements v1.5.6.

- By confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record to confirm the applicant's practical control over the FQDN. This way of validation conforms to section 3.2.2.4.7 of the Baseline Requirements v 1.5.6.

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.

GDCA does not issue EV SSL certificate for an IP address.

4. 邮箱地址验证

通过发送电子邮件的方式确认：

(1) GDCA 向该邮箱发送校验信息,要求该邮箱用户根据校验信息在一定的时间内回复邮件；

(2) GDCA 收到该邮件后，进行审核确认，完成鉴别流程。

4. Confirmation of e-mail address

Email address can be confirmed via sending e-mail:

(1) GDCA sends the check information to e-mail account address and requires the user of this account to reply an e-mail according to these information within a certain period.

(2) After receiving the e-mail, GDCA will check the validity of it and finish the authentication process.

5. 机构商业名称验证

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。

5. Verification of DBA/Tradename

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.

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

EV 证书不接受个人申请。

EV certificate is not applicable to individuals.

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

EV 证书中所有包含的订户信息都应进行验证。

All subscribers' information in EV certificate should be verified.

3.2.5. 授权确认 Validation of Authority

当机构订户授权经办人办理证书业务时，GDCA 进行如下验证：

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

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

The following verification should be conducted while the representative of organization subscriber applying for certificate:

1. Confirming the organization from third-party identity verification service or database, documents issued by government.
2. Using telephone, postal letter with return receipt, employment proof document or any equivalent way to confirm that the person belongs to above organization and his/her behavior is

authorized by these organization.

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

3.2.6. 互操作准则 Criteria for Interoperation

对于其他的电子认证服务机构，可以与 GDCA 进行互操作，但是该电子认证服务机构的 CPS 必须符合 GDCA CP 要求，并且与 GDCA 签署相应的协议。

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

如果国家法律法规对此有规定，GDCA 将严格予以执行。

截至目前，GDCA 未签发任何交叉证书。

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

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

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

To date, GDCA has not issued any cross certificates.

3.2.7. 数据来源的准确性 Data Source Accuracy

在将任何数据来源作为可依赖数据来源使用之前，GDCA 对该来源的可依赖性、准确性及防伪造或更改性进行评估，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不超过证书签发前 825 天，则 GDCA 可使用该数据及文件。

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

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

GDCA may use the documents and data to verify certificate information, provided that it obtained the data or document no more than 825 days prior to issuing the certificate.

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

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

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

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

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

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

密钥更新会造成使用原密钥对加密的文件或数据无法解密，因此，订户在申请密钥更新前，必须确认使用原密钥对加密的文件或者数据已经解密，由此造成的损失，GDCA 将不承担责任。

The renewal of the secret key will cause that the original secret key is unable to decrypt the files or data. Therefore, the subscriber should make sure the encrypted documents or data have been decrypted before they apply for the secret key’s updating. GDCA shall not assume any responsibility incurred by failure of decryption by the renewal of the secret key.

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

EV 证书吊销后不能进行密钥更新。

Re-key/renewal after revocation of EV certificate is not permitted.

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

当 GDCA 或注册机构有充分的理由吊销订户的证书时，有权依法吊销证书，这种情况无须进行鉴证。如果订户主动要求吊销证书，则按照本 CPS 第 3.2 节描述进行身份鉴别。

GDCA or RA can revoke a certificate based on sufficient reason without authentication. Subscriber who requests to revoke a certificate will follow CPS section 3.2.

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

GDCA 自行担任 EV 证书的 RA，不再另行设立 RA。

GDCA will serve as RA by itself, rather than will 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

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

Entities of certificate request are organizations with independent legal person qualification (such as

administrative organizations, institutions, social organizations, people's organizations and other organizations).

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

EV 证书注册操作符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南的要求。

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

申请者应向 GDCA 递交 EV 证书申请表及相应证明文件，此行为即意味着申请者已经了解和接受上述内容。

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。

EV certificate registration operation complies with requirements of guidelines published by CA/ browser Forum at www.cabforum.org.

Applicant should learn subscriber’s agreement, provisions agreed in EV CP and this CPS and other files in advance. Especially, applicant should focus on related content about the certificate applicable scope, rights, obligations and warranties.

Applicant should submit an EV certificate application form and corresponding documents to GDCA. All of above mean that applicant has learned and accepted the contents.

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

GDA shall ensure the consistency between certificate application information and identification which subscribers provided and bear corresponding responsibilities of review.

4.2. 证书申请处理 Certificate Application Processing

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

当 GDCA 及其注册机构接受到订户的证书申请后，应按本 CPS3.2.2、3.2.3、3.2.4 及 3.2.5 的要求，对订户进行身份识别与鉴别。

GDCA 验证申请者提交的申请材料后，根据验证结果决定接受、拒绝该申请或要求申请者补充递交相关材料。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。

在证书签发前，若 GDCA 根据 CPS 3.2 指定来源获得的数据或证明文件不超过 825 天且该信息未发生变化，则 GDCA 可使用该数据或证明文件，核实证书中的信息。

After GDCA and its registration agencies receive the subscriber's certificate application, they should perform identity recognition and verification of identification over the subscriber according to the requirements of CPS 3.2.2, 3.2.3, 3.2.4 and 3.2.5.

After verifying the application materials submitted by applicants, GDCA will accept or reject this application or require the applicant to submit supplemental related materials according to the verification result.

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

GDCA may use the documents and data provided in section 3.2 to verify certificate information, provided that it obtained the data or document from a source specified under section 3.2 no more than 825 days prior to issuing the certificate, and provided that no changes occurred to the documents and data within such time period.

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

完成 4.2.1 识别与鉴别的执行后，如果用户满足相应要求，则视为 GDCA 已经批准该证书请求，申请者即成为 GDCA 的 EV 证书订户；否则应拒绝证书申请。

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吊销的证书，建立和维护 EV 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。

After completing the execution of identification and authentication in Section 4.2.1, if the user meets related requirements, it means that GDCA has approved this certificate request. Applicant becomes a subscriber of GDCA EV certificate. Otherwise, GDCA shall reject the certificate application.

If application is prohibited clearly by laws and regulations, or GDCA considers that there is highly risk to approve the application, GDCA shall reject it. GDCA establishes and maintains a list of high risk EV certificate applicants according to the list provided by anti-phishing alliance, antivirus vendor or related alliance, government agencies which are responsible for network security affairs and other third party, or the disclosure of information through public media reports, or previously rejected certificate requests by GDCA due to suspected phishing or other fraudulent usage or concerns. GDCA will query information from the list during accepting certificate application. If the applicants appear in this list, GDCA will reject their application directly.

对于已签发的 EV 证书，也将会定期根据列表予以复核，一旦发现证书持有人出现在列表中，GDCA 有权撤销该证书或采取适当机制进行谨慎处理。

对于法律法规、国家政府部门、行业监管部门或当地政府明确禁止从事商业活动或其它公开活动的机构，GDCA 有权拒绝为其签发 EV 证书。此外，如果证书申请相关人员受到法律法规、国家或地方政府的相关限制，GDCA 可不予受理由其参与的 EV 证书申请事宜。

For the EV certificates which had been issued, GDCA will also review them regularly according to the list described above. Once the holder of the certificate is found in the list, GDCA gets the right to revoke the certificate or take appropriate mechanisms for careful handling.

For the authorities which laws and regulations, national government departments, industry supervision department or local government clearly prohibit from engaging in commercial activities or other public activities, GDCA gets the right to refuse to issue EV certificate to them. In addition, if relevant personnel of certificate application suffers from the relevant restrictive of laws and regulations, state or local government, GDCA can refuse to their EV certificate application process.

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

GDCA 注册机构成功完成了证书申请所有必需的确认步骤并提交证书请求后，GDCA 通过发行正式证书来批准证书申请，一旦证书被发行，CA 将没有继续的责任去调查证书信息的正确性。

如果符合下述条件，注册机构（RA）可以批准证书申请：

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

After GDCA's registration authority completes verification steps for the certificate application successfully and submits a certificate request, if GDCA issues official certificates, which means GDCA approves certificate application. Once the certificate is issued, GDCA shall not have the responsibility for inspecting the accuracy of the certificate information.

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

1. The application shall completely meet the requirements from CPS 3.2 regarding the subscriber's identification information and authentication.

2. Applicant accepts or has no opposition regarding the content or requirements of the subscriber's agreement.

3. Applicant has paid already in accordance with the provisions.

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

如果发生下列情形，GDCA 拒绝证书申请：

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

GDCA refuses the certificate application in case of the following situations:

1. The application does not meet the specifications of subscriber's identification and authentication in CPS 3.2.
2. The applicant can't provide the required identity documents.
3. The applicant objects or can't accept the relevant content or requirements of the subscriber's agreement.
4. The applicant has not paid or is not able to pay the appropriate fees.
5. The requested certificates contain a new gTLD under consideration by ICANN (The Internet Corporation for Assigned Names and Numbers).
6. GDCA or RA considers that the approval of the application will bring the dispute, legal disputes or losses to GDCA.

对于拒绝的证书申请，GDCA 通知申请者证书申请失败。

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

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

GDCA 应在合理的期限内完成证书申请处理。

GDCA should finish processing certification applications in a reasonable period.

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

对于 GDCA 颁发的满足 CA/浏览器论坛 EV Guidelines、Baseline Requirements 要求

的公共可信任的 SSL 证书，从 2017 年 7 月 1 日起，GDCA 将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，在此之前，GDCA 对 SSL 证书申请不做 CAA 检查。

GDCA 根据 RFC6844（经勘误表 5065 修订）的规定处理“issue”、“issuewild”及“iodef”的属性标签：若“issue”、“issuewild”标签中不包含“gdca.com.cn”，则 GDCA 不签发对应的证书；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）域名所在区域不存在指向 ICNNA 根区域的 DNSSEC 验证链。

For the publicly trusted SSL certificates issued by GDCA and conform to the EV Guidelines and Baseline Requirements of the CA/Browser Forum, from July 1, 2017, GDCA will check the CAA records and follow the processing instructions found for each dNSName in the subjectAltName extension of the certificate to be issued, and GDCA will not perform the CAA check for the SSL certificate requests before July 1, 2017.

GDCA processes "issue", "issuewild", and “iodef” property tags according to RFC6844 as amended by Errata 5065: 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) the domain's zone does not have a DNSSEC validation chain to the ICANN root.

4.3. 证书签发 Certificate Issuance

4.3.1. 电子认证服务机构（CA）的行为 CA Actions

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

CA 将在证书申请被批准后生成并签发证书。CA 为申请人生成和签发的证书基于其在证书申请中被批准的信息。签发证书的操作符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 12 部分的要求。

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

The certificate will be generated and issued if the application is approved by CA. The contents of

these certificates are based on the approved information on the certificate application. The operations of certificate issuance are in compliance with requirements of Section 12 guidelines published by CA/Browser Forum at www.cabforum.org.

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

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

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

4.4. 证书接受 Certificate Acceptance

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

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

1. Subscribers access to specialized GDCA certificate service website, then download certificate to the certificate carrier, that means subscriber totally accepted the certificate after it has been downloaded.
2. When RA of GDCA downloads the certificate on behalf of subscriber, the downloaded certificate will be kept in digital certificate carrier. Once the subscribers accept the certificate carrier, the subscribers accept the certificate.
3. Subscribers fail to oppose or conduct the operation of objection over the certificates or the content of certificates.

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

订户接受证书后，GDCA 在 24 小时内将该订户证书发布到 GDCA 的目录服务系统。

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

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

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

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

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

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

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

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

订户在提交了证书申请并接受了 GDCA 所签发的证书后，均视为已经同意遵守与 GDCA、依赖方有关的权利和义务的条款。订户接受到数字证书，应采取合理措施妥善保存其证书对应的私钥避免未经授权的使用。

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

对于 EV 代码签名证书，不存在一个证书对应多个软件对象。

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

After the subscribers have submitted certificate application and received certificates issued by GDCA, they are deemed to have agreed to comply with the terms of GDCA, relying party related rights and obligations. The subscriber who receives the certificate shall properly take appropriate measures to keep the corresponding private key to the certificate from unauthorized use.

Subscriber should protect his/her private key from unauthorized use, and do not use expired or

revoked certificates. In addition, the private key should not be archived.

For EV CodeSigning certificates, a certificate should not be related to multi-software at the same time.

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

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

当依赖方接收到加载数字签名的信息后，有义务进行以下确认操作：

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

以上条件不满足的话，依赖方有责任拒绝签名信息。

当依赖方需要发送加密信息给接受方时，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密。依赖方应将加密证书连同加密信息一起发送给接受方。

When the relying party has received the message with digital signature, the party has the obligation to carry out the following operations to confirm:

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

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

When the relying party needs to send an encrypted message to the receiving party, the party must first obtain the encryption certificate of receiving party through proper channels, and then encrypt the information using public key of the certificate. The relying party should send the encryption certificate and encrypted information to receiving party.

4.6. 证书更新 Certificate Renewal

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

GDCA 不提供 EV 证书更新服务。

GDCA does not provide EV certificate renewal service.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

4.7. 证书密钥更新 Certificate Rekey

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

GDCA 的证书密钥更新包括但不限于以下情形：

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

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

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

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

请求证书密钥更新的实体为证书订户。

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

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

参照 CPS 第 3.3 节的规定对证书密钥更新进行用户身份鉴别和识别。

参照 CPS 第 4.3 节的规定对证书进行签发。

Authentication and identification of subscriber identity are done for re-key according to CPS section 3.3.

Certificates are issued according to CPS section 4.3.

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

同本 CPS 第 4.3.2 节。

See CPS section 4.3.2.

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

同本 CPS 第 4.4.1 节。

See CPS section 4.4.1.

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

同本 CPS 第 4.4.2 节。

See 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 CPS 第 4.4.3 节。

See CPS section 4.4.3.

4.8. 证书变更 Certificate Modification

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

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

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

4.9. 证书吊销和挂起

Certificate Revocation and Suspension

证书撤销和状态查询操作符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 13 部分的要求。

The operations of Certificate revocation and status query are in compliance with requirements of Section 13 guidelines published by CA/Browser Forum at www.cabforum.org.

4.9.1. 证书吊销的情形

Circumstances for Revocation

4.9.1.1. 订户证书吊销的原因 Reasons for Revoking a Subscriber Certificate

当发现以下的情况，证书必须被吊销：

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的订户私钥遭到了损害，或不再符合 Baseline Requirements 第 6.1.5 节及第 6.1.6 节；
4. GDCA 获得了证书遭到误用的证据；
5. 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；
6. 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吊销了域名注册人使用域名的权力，域名注册人与申请人的相关许可及服务协议被终止，或域名注册人未成功更新域名）；
7. 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；；
8. GDCA 获悉证书中所含信息出现重大变化；
9. GDCA 获悉证书的签发未能符合 Baseline Requirements 要求，或 GDCA 的 CP 或

CPS；

10. GDCA 认为任何出现在证书中的信息不准确、不真实或具有误导性；
11. 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吊销服务；
12. GDCA 依据 Baseline Requirements 签发证书的权力失效，或被撤销或被终止，除非其继续维护 CRL/OCSP 信息库；
13. GDCA 获悉用于签发证书的中级 CA 的私钥遭到了可能的损害；
14. GDCA 的 CP 或 CPS 要求吊销订户证书；
15. 证书的技术内容或格式为应用软件供应商或依赖方（例如，CA/Browser 论坛可能认为加密或签名算法或密钥长度导致了不可接受的风险而弃用，且此证书应在规定时间内由 GDCA 吊销及替换）带来了不可接受的风险。
16. 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；
17. GDCA 已经履行催缴义务后，订户仍未缴纳服务费。

Certificates must be revoked 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 no longer complies with the Baseline Requirements sections 6.1.5 and 6.1.6;
4. GDCA obtains evidence that the certificate was misused;
5. GDCA is made aware that a subscriber has violated one or more of its material obligations under the subscriber agreement and CP/CPS;
6. GDCA is made aware of any circumstance indicating that use of a fully-qualified domain name or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a domain name registrant’s right to use the domain name, a relevant licensing or services agreement between the domain name registrant and the applicant has terminated, or the domain name registrant has failed to renew the domain name);
7. GDCA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name;
8. GDCA is made aware of a material change in the information contained in the certificate;
9. GDCA is made aware that the certificate was not issued in accordance with Baseline Requirements or GDCA’s CP or CPS;

10. GDCA determines that any of the information appearing in the certificate is inaccurate, unreal or misleading;
11. GDCA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
12. GDCA's right to issue certificates under the Baseline Requirements expires or is revoked or terminated, unless it has made arrangements to continue maintaining the CRL/OCSP repository;
13. GDCA is made aware of a possible compromise of the private key of the subordinate CA used for issuing the certificate;
14. Revocation is required by GDCA's CP and/or CPS;
15. The technical content or format of the certificate presents an unacceptable risk to application software suppliers or relying parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such certificates should be revoked and replaced by GDCA within a given period of time);
16. The fulfillment of the obligations in the CPS is delayed or encounters force majeure, such as natural disasters, computer or communications failures, changes of laws and regulations, government actions or other causes beyond the reasonable control, causing threats to the information of others; or
17. Subscribers fail to pay the service fees after GDCA performed the obligations of notifying the subscribers to pay..

4.9.1.2. 中级 CA 证书的吊销原因 Reasons for Revoking a Subordinate CA Certificate

若出现以下情况中的一种或多种，GDCA 应在 7 天之内吊销中级 CA 证书：

1. GDCA 获得了证据，证明与证书公钥对应的中级 CA 私钥遭到了损害，或不再符合 Baseline Requirements 第 6.1.5 节及第 6.1.6 节的相关要求；
2. GDCA 获得了证书遭到误用的证据；
3. GDCA 获悉证书的签发未能符合 Baseline Requirements 要求，或中级 CA 未能符合 CP/CPS；
4. GDCA 认为任何出现在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吊销服务；
6. GDCA 依据 Baseline Requirements 签发证书的权力失效，或被撤销或被终止，除非其继续维护 CRL/OCSP 信息库；
7. GDCA 的 CP/CPS 要求吊销中级 CA 证书；
8. 证书的技术内容或格式为应用软件供应商或依赖方（例如，CA/Browser 论坛可能认为加密或签名算法或密钥长度导致了不可接受的风险而弃用，且此证书应在规定时

间内由 GDCA 吊销及替换）带来了不可接受的风险。

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 Baseline Requirements of Sections 6.1.5 and 6.1.6;
2. GDCA obtains evidence that the certificate was misused;
3. GDCA is made aware that the certificate was not issued in accordance with Baseline Requirements or that subordinate CA has not complied with the GDCA CP or CPS;
4. GDCA determines that any of the information appearing in the certificate is inaccurate, unreal or misleading;
5. GDCA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
6. GDCA's right to issue certificates under Baseline Requirements expires or is revoked or terminated, unless GDCA has made arrangements to continue maintaining the CRL/OCSP Repository;
7. Revocation is required by GDCA's CP and/or CPS;
8. The technical content or format of the certificate presents an unacceptable risk to application software suppliers or relying parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such certificates should be revoked and replaced by GDCA within a given period of time).

4.9.2. 请求证书吊销的实体 Who Can Request Revocation

请求证书吊销实体为订户、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 有合理理由吊销证书。

The subscribers, RA, GDCA, or judicial officials authorized by judicial institutions can initiate revocation. Additionally, relying parties, application software suppliers, anti-virus organizations and other third parties may submit certificate problem reports informing GDCA of reasonable grounds to revoke the certificates.

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

4.9.3.1. 订户主动提吊销申请 The subscriber actively proposed to revocation application.

1. 订户向 GDCA 提交吊销申请表和身份证明材料，同时说明吊销原因；
2. GDCA 按照本 CPS 第 3.4 节的规定进行证书吊销请求的鉴别；
3. GDCA 在接到吊销请求后的 2 个工作日内完成证书吊销；
4. GDCA 完成吊销后及时将其发布到证书吊销列表；
5. GDCA 通过电话、邮件等适当方式，通知订户证书被吊销及被吊销的理由；
6. GDCA 提供 7*24 小时的证书吊销申请服务，订户可通过以下方式申请注销：
   - 电话号码：95105813
   - E-mail: webtrustreport@gdca.com.cn

1. Subscriber submits application form of revocation and documents of identity confirmation to GDCA. Meanwhile, subscriber should provide reasons of revocation.
2. GDCA makes authentication of certificate revocation request according to CPS section 3.4.
3. GDCA completes certificate revocation within 2 working days after receiving revocation request.
4. After the completeness of revocation, GDCA releases it to CRL promptly.
5. GDCA notifies to subscriber that the certificate was revoked and the revoked reason by appropriate means, such as telephone, mail, and etc.
6. GDCA offers 24x7 certificate revocation requests service, and subscribers may request the revocation of a certificate through the following ways:
   - Call: 95105813
   - E-mail to: webtrustreport@gdca.com.cn

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

1. 当 GDCA 有充分的理由确信出现本 CPS 第 4.9.1 节中的情况时，须经过 GDCA 安全策略委员会批准后方可进行；
2. 在 GDCA EV Root 证书或 EV 中级 CA 证书相对应的私钥出现安全风险时，经国家电子认证服务主管部门批准后可直接进行证书撤销；
3. 在证书吊销后，GDCA 或注册机构将通过适当的方式，包括邮件、电话等，通知最终

订户证书已被吊销及被吊销的理由。若未能联络订户时，在必要的情况下，GDCA 对吊销的证书将通过网站进行公告；

4. GDCA 提供 7*24 小时的 EV 证书问题报告和处理流程。

GDCA can revoke subscriber's certificate with the occurrence of circumstances described in CPS section 4.9.1 after the approval of GDCA Security Policy Committee.

GDCA can revoke the certificate with the occurrence of security risk for private key of GDCA EV Root certificate or EV Subordinate CA certificate after the approval of state's electronic authenticate service administrative department.

After the certificate revocation, GDCA or RA will use appropriate ways, including mail, phone, fax to notify the final subscriber that the certificate has been revoked and the reason why to be revoked. If GDCA can't contact subscriber, in case of need, GDCA will notice the revoked and suspended certificates on the website.

For EV certificate, GDCA provides 7*24 hours problem reports and handling procedures.

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

GDCA 本身证书的吊销，必须经过相关监管部门确定后才可以进行。

GDCA's certificates will be revoked only after the approval from the regulatory authorities concerned.

4.9.4. 问题和报告处理机制 Processing Mechanism of Problems and Reports

订户应在证书对应的私钥出现或疑似泄漏、被破解或被滥用时，应立即告知 GDCA，最长不超过 24 小时。GDCA 在接到订户报告后应在 24 小时内，对已经接受报告的证书进行调查和决定是否撤销或采取其他适当的行动处理机制。

GDCA 建立并保持 7*24 小时的 EV 证书问题报告和受理机制，任何订户、依赖方、应用软件供应商或其他第三方发现证书可能存在问题、私钥出现或怀疑出现泄漏、证书滥用、或其他与 EV 证书相关的舞弊、泄漏、滥用或不正当行为时，均可向 GDCA 进行报告或投诉。报告方式如下：

- 电话号码：95105813
- E-mail: webtrustreport@gdca.com.cn

When corresponding private key of subscriber certificate has occurred suspected leakage, broken or abuse, subscriber should immediately notify GDCA no longer than 24 hours. After receiving the report from subscribers, GDCA should make investigation for the certificate which has been

reported and decide whether to revoke it or take other appropriate action processing mechanism within 24 hours.

GDCA establishes and maintains reports 7*24 hour problem report and acceptance mechanism for EV certification, any subscriber, relying party, application software provider or other third-party who find a certificate with fraud, leakage or suspected leakage of private key, abuse and other problems can report or complaint to GDCA. The ways to report are as follows:

- Telephone number: 95105813
- E-mail: webtrustreport@gdca.com.cn

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吊销证书：

（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 EV 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。

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

(1) The nature of the alleged problem;

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

(3) The entity making the reports or complaints;

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

(5) Compliance with existing laws and regulations.

4.9.5. 吊销请求宽限期 Revocation Request Grace Period

如果出现密钥泄露或有泄露嫌疑等事件，吊销要求必须在发现泄密或有泄密嫌疑 8 小时以内提出。其他吊销原因的吊销要求必须在变更前的 48 小时内提出。

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

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

GDCA 处理吊销请求的周期为 24 小时。

The cycle of GDCA processes revocation request is 24 hours.

4.9.7. 依赖方检查证书吊销的要求 Revocation Checking Requirements for Relying Parties

GDCA 提供在线吊销状态查询，依赖方可在 GDCA 的网站上进行查询。

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

4.9.8. CRL 发布频率 CRL Issuance Frequency

对于订户证书，GDCA 的 CRL 发布周期为 24 小时，即在 24 小时内发布最新 CRL，且 nextUpdate 字段的值不超出 thisUpdate 值的 10 天以上。

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

CRL 签发频率符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第 13 部分的要求。

For the subscriber certificates, GDCA updates and publishes certificate revocation list (CRL) every 24 hours, and the value of the nextUpdate field is not more than ten days beyond the value of the thisUpdate field.

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

CRL Issuance frequency meets requirements of Section 13 guidelines published by CA/Browser Forum at www.cabforum.org.

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

GDCA 的 CRL 发布最大滞后时间为发布周期之后的 24 小时内。

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

4.9.10. 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.

4.9.11. 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。

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

对于未签发的证书的状态查询请求，GDCA 不返回“good”状态 。

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

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

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

For 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.

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

GDCA 不提供吊销信息的其他发布形式。

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

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

除本 CPS 中第 4.9.1 节规定的情形外，当订户或注册机构的证书密钥已经失密或者可能已经失密时，必须及时向 GDCA 提出证书吊销请求。如果 CA 的密钥（根 CA 或中级 CA 密钥）安全被损害或者怀疑被损害，应该在合理的时间内用合式的方式及时通知订户和依赖方。

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

4.9.14. 证书挂起的情形 Circumstances for Suspension

不适用。

Not applicable.

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

不适用。

Not applicable.

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

不适用。

Not applicable.

4.9.17. 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。

对于被吊销的证书，GDCA 在证书到期前不删除其在 CRL 中的吊销记录。GDCA 不删除 CRL 中代码签名证书的吊销记录。

GDCA 不删除 OCSP 服务器中的吊销记录。

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

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

GDCA does not remove the revocation records in the OCSP responder.

4.10.2. 服务可用性 Service Availability

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

证书状态服务的可用性符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南第 13 部分的要求。

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

The availability of certificate status service meets requirements of Section 13 guidelines published by CA/Browser Forum at www.cabforum.org.

4.10.3. 可选特征 Operational Features

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

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

4.11. 订购结束 End of Subscription

订购结束包含以下情况：

1. 证书到期后没有进行更新；
2. 证书到期前被吊销。

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注销，并按照 CRL 发布策略进行发布；GDCA 详细记录吊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。

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

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

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

4.12. 密钥托管与恢复 Key Escrow and Recovery

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

GDCA 不得托管任何 EV 证书订户的私钥，因此也不提供密钥恢复服务。

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

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：

1. GB/T 25056-2010《信息安全技术 证书认证系统密码及其相关安全技术规范》
2. 国密局[2010]7 月《电子政务电子认证基础设施建设要求》
3. GB50174-2008《电子信息系统机房设计规范》
4. GB6650-1986：《计算机机房用活动地板技术条件》
5. GB2887-2011《计算机场地通用规范》
6. GB30003-93《电子计算机机房施工及验收规范》
7. GB50222-95《建筑内部装修设计防火规范》
8. GB50116-98《火灾自动报警系统设计规范》
9. GB50057-94《建筑物防雷设计规范》
10. GB5054-95《低压配电设计规范》
11. GB/J19-87《采暖通风与空气调节设计规范》
12. SJ/T10796-1996《计算机机房用活动地板技术条件》
13. YD/T754-95《通讯机房静电防护通则》

1. GB/T 25056-2010 “Information security techniques- Specifications of cryptograph and th e related security technology for certificate authentication system”.
2. State Cryptography Administration [2010] July “Construction Requirements for electronic Authentication Infrastructure of E-government”.
3. GB50174-2008 “Code for design of electronic information System Room”.
4. GB6650-1986 “Specification for raised floor of computer room”.
5. GB2887-2011 “Specification for computer field”
6. GB30003-93 “Construction and acceptance test code for electronic computer room”.

7. GB50222-95 “CCode for Fire Prevention in Design of Interior Decoration of Buildings”.
8. GB50116-98 “Code for design of automatic fire alarm system”
9. GB50057-94 “Design code for protection of Structures against lightning”
10. GB5054-95 “Code for design of low voltage electrical installations”
11. GB/J19-87 “Code for design Of heating ventilation and air conditioning”
12. SJ/T10796-1996 “Specification for raised floor of computer rooms”
13. YD/T754-95 “General rules for electrostatic protection of communication rooms”

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

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

5.1.1.1. 公共区域 Public Area

公共区包括入口、大堂、保安室，部署各配套设施和监控设备，进入公共区域都必须登记。

Public area includes the entrance, lobby, security room and etc., deployed with various supporting facilities and monitoring devices. Any individuals must be registered when access to the public area.

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，需要同时使用身份识别卡和指纹鉴别才可以进入，人员进出操作区要有日志记录。从该层开始，所有的墙体都应采用高强度防护墙。

Operation area is a working place for RA operators and administrators. Anyone who wants to enter the operation area needs to use identification card and fingerprint identification at the same time. Every access behavior to the operation area has been well recorded. From this level of areas, all the walls should be strengthened by high strength protective wall.

5.1.1.3. 管理区 Management Area

管理区安装 RA 管理控制台，CA 管理、签发、审计控制台，网络管理、监控控制台，是 RA 和 CA 管理员、审计员和网络安全员的工作区，只允许管理区规定的管理人员进入，需要两个管理员同时使用身份识别卡和指纹鉴别才可以进入。

Management area is a working area for RA and CA administrators, auditors and network security officers, installed with the RA management console, CA consoles of management, issue, and audit, and consoles of network management and monitor. Only authorized and specified administrators have the rights to access this area. Enter this area needs two administrators to use identification card and fingerprint identification at the same time.

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身份识别卡和指纹鉴别才可以进入。

Service area is installed with LDAP servers, OCSP servers, RA register servers and other related devices. Only authorized and specified administrators have the rights to access this area. Entering this area needs two administrators to use identification card and fingerprint identification at the same time.

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身份识别卡和指纹鉴别才可以进入。密码柜也安放在核心区，存放保密资料。

Core area, a shielding zone with high strength steel security doors, is mainly installed with CA signature servers, CA database servers, KM key management servers, timestamp servers and other core devices. Only authorized and specified administrators have the rights to access this area. Enter this area needs two administrators to use identification card and fingerprint identification at the same time. The password ark for storing confidential information is also placed in the core area.

5.1.2. 物理访问 Physical Access

GDCA 机房内设有 9 扇门安装电子门禁系统和 1 个物理侵入报警器，对门禁系统进行监控，实时读取门禁记录的资料，并对门禁系统设置权限。该系统能实时读取进出门

资料，并有门开超时报警。工作人员都需使用身份识别卡或结合指纹才能进出，并且进出每一道门都有时间记录和相关信息提示，服务区与核心区需要两个管理员同时使用身份识别卡和指纹鉴别才可以进入，机房工作人员按照机房日常工作规范，每月对门禁记录进行整理归档，保留一年的门禁记录。

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。

In the data center of GDCA, it has 9 doors installed with electronic access systems and one physical intrusion alarm. The electronic access systems are monitored, with real-time access records to set permissions of access, and can set an alarm when the doors are opened over time. The staff is required to use the identity card and fingerprint to open every door, and each access behavior has been recorded with time-stamp and related notice. Enter the service area and core area, two administrators need to use ID cards and fingerprint identification at the same time before entering the room. According to daily working specification, the specific personnel will archive the access records on a monthly basis, and retained for one year at least.

Physical access controls includes the following aspects:

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

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

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

5.1.3. 安防监控 Security Monitoring

根据机房动力环境保安监控系统的要求，本机房环境监控系统包括的子系统有：配电检测子系统、UPS 检测子系统、空调设备检测子系统、新风机检测子系统、温湿度检

测子系统、漏水监测子系统、消防子系统、门禁子系统、图像监控子系统。对基础设施设备、机房环境状况、安防系统状况进行 7*24 小时实时监测，为满足故障诊断、事后审计的需要，监控记录保留时间为 6 个月以上。

According to the requirement of data center power and environment security monitoring system, it includes electronic detection subsystem, UPS detection subsystem, air conditioning equipment detection subsystem, fresh air machine detection subsystem, temperature and humidity detection subsystems, water leakage monitoring subsystem, fire control subsystem, access control subsystem and image monitoring subsystem. The system carries out real-time monitoring of infrastructure equipment status, data center environment condition and the security system status within 7*24 hours. In order to meet the need of fault diagnosis and post audit, monitor records will be retained for more than 6 months.

5.1.4. 电力与空调 Power and Air Conditioning

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

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

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

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

5.1.5. 水患防治 Water Exposures

为防治水害对机房的威胁，GDCA 在机房的空调室内设置漏水报警系统。漏水报警

检测绳在空调周围设置，一旦发生水患立即报警，通知有关人员采取应急措施。同时在沿外墙四周做排水沟及泄水地漏，一旦发生水患，水能立即排泄出去，并对所有外窗已做封闭处理。

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

5.1.6. 火灾防护 Fire Prevention and Protection

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

在自动状态下，当防护区发生火警时，火灾报警控制器接到防护区两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。

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

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

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

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

5.1.7. 介质存储 Media Storage

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

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

5.1.8. 废物处理 Waste Disposal

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

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

5.1.9. 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、管理和吊销等涉及密钥操作的职位都被 GDCA 视为可信角色。这些角色包括但不限于：密钥和密码设备的管理人员、系统管理人员、安全审计人员、业务管理人员及业务操作人员等，具体岗位名称和要求以 GDCA 的岗位说明为准。

In the process of electronic authentication service provided by GDCA, a person who can essentially affect the processes of certificate issuance, usage, management and revocation, and other related positions which are involved in key operation is considered as trusted roles. The trusted roles include but are not limited to: key and cryptographic equipment administrators, system administrators, security audit administrators, business administrators and business operators, etc. The specific job names and requirements shall be subject to, the GDCA job descriptions prevail.

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：

- ◆ 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
- ◆ 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
- ◆ 审核和签发证书：需要 2 个可信人员共同完成

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

- ◆ For operation and storage of the key cryptographic equipment, it requires at least three of five trusted persons to operate.
- ◆ For background operation of the certificate issuance system, it requires at least two of three trusted persons to operate.
- ◆ For review and issuance of the certificate, it requires two trusted persons to operate.

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

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

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

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

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

a） 证书业务受理

b） 证书或 CRL 签发

c） 系统工程与维护

d） CA 密钥管理

e） 安全审计

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

- The acceptance of the certificate businesses
- The issuance of certificates or CRLs
- System Engineering and Maintenance
- CA key management
- Security auditing

5.3. 人员控制 Personnel Controls

人员控制符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 14.1 部分的要求。

Personnel control meets requirements of Section 14.1 guidelines published by CA/Browser Forum at www.cabforum.org.

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。

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

The qualification requirements of person who undertakes trusted role in GDCA are as follows:

1. Good social and working background.
2. Complying with state's laws and regulations. Obeying GDCA's unified arrangement and management.
3. Complying with the GDCA related security management norms, regulations and specifications.
4. Having good personalities and working attitudes, with good working experience.
5. A good team player.
6. No illegal and criminal records.

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

5.3.2. 背景审查程序 Background Check Procedures

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

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

背景调查分为：基本调查和全面调查。

基本调查包括对工作经历，职业推荐，教育，社会关系方面的调查。

全面调查除包含基本调查项目外还包括对犯罪记录，社会关系和社会安全方面的调查。调查程序包括：

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

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

c)在背景调查中，对发现以下情形的人员，可以直接拒绝其成为可信人员的资格：

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

d) 用人部门通过现场考核、日常观察、情景考验等方式对其考察。关键和核心岗位的人员通过录入考察期后，还需要额外期限的考察。根据考察的结果作出相应的安排。

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

Background review including: basic review and full review.

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

Full review includes reviewing criminal records, social relation and social security apart from the basic review.

The review procedure includes:

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

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

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

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

d) The HR department checks candidates through on-site assessment, daily observation, situational test and other methods. After the staff of key and core position has passed the review period, extra inspection must be required. Appropriate arrangement is made according to the investigation result.

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

5.3.3. 培训要求 Training Requirements

GDCA 根据可信角色的职位需求，给予相应的岗前培训，综合培训内容如下：

- GDCA 运营体系；
- GDCA 技术体系；
- GDCA 安全管理策略和机制；
- 岗位职责统一要求；
- PKI 基础知识；
- 身份验证和审核策略和程序；
- 灾难恢复和业务连续性管理；
- CP、CPS 政策及相关标准和程序；
- GDCA 管理政策、制度及办法等；
- 国家关于电子认证服务的法律、法规及标准、程序；

其他需要进行的培训等等。

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

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

此外，对于证书操作员和审核员，GDCA 定期开展工作职责所需要的培训，包括岗位职责、事件和损坏的报告处理流程、灾难恢复和业务连续性管理流程等。在新系统上线或认证系统的重要更新或升级时，对操作人员和审核人员也需进行相应的培训。

In addition, for certificate operator and auditor, GDCA carries out required training for working duties

regularly, including job duties, events and damage report process, disaster recovery and business continuity management process. In online of new system or significant updates or upgrades of certification system, GDCA should carry out corresponding training for operator and auditor.

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，每年至少接受 GDCA 组织的培训一次。对于认证系统运营相关的人员，每年至少进行一次相关技能和知识培训。此外，GDCA 将根据机构系统升级、策略调整等要求，不定期的要求人员进行继续培训。

For persons acting as trusted roles or other important roles, they should be trained at least once a year by GDCA. Related personnel for operating authentication system should have the training of relevant skills and knowledge at least once a year. In addition, GDCA will provide ongoing training for employees irregularly according to system upgrade, strategy adjustment and other requirements.

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

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

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

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

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

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

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

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

- 人员档案的备案管理；
- 具有 1 年以上相关业务工作经验；
- GDCA 提供统一的岗前培训辅导和再培训要求，培训内容包括但不限于 GDCA 证书受理规则和电子认证业务规则。

For persons who do not belong to the GDCA but participate in the relevant works for GDCA businesses, such as business personnel of business branch organization, management personnel and other independent contractors, GDCA has requirements are as follows:

- Record management of personnel profiles
- With more than 1 year relevant work experience
- GDCA provides unified training and retraining, includes but not limited to the GDCA certificate acceptance rules and electronic certification business rules.

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

在培训或再培训期间，GDCA 提供给员工的培训文档包括但不限于以下几类：

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

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

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

5.4. 审计日志程序 Audit Logging Procedures

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

所有发生在 GDCA 的重大安全事件都会自动地打上时间印章并记录在审计跟踪档案中，这些记录，不论是手动生成或者是系统自动生成，都应该包含以下信息：

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

All major security incidents occurred in GDCA will be logged with the time-stamp and recorded in the audit trail records automatically. Regardless of manual or automatic generation, these records should contain the following information:

1. The date and time of the event
2. Sequence number for the record
3. Type of record
4. Record source
5. Event recording entity

这些事件包括但不限于：

1. 密钥生命周期内的管理事件，包括密钥生成、备份、存储、恢复、使用、吊销、归档、销毁、私钥泄露等；
2. 密码设备生命周期内的管理事件，包括设备接收、安装、卸载、激活、使用、维修等；
3. 证书申请事件，包括订户接受订户协议，接受申请的单位、申请资料的验证、申请及验证资料的保存等；
4. 证书生命周期内的管理事件，包括证书的申请、批准、更新、吊销等；系统安全事件，包括：成功或不成功访问 CA 系统的活动，对于 CA 系统网络的非授权访问及访问企图，对于系统文件的非授权的访问及访问企图，安全、敏感的文件或记录的读、写或删除，系统崩溃，硬件故障和其他异常；
5. 防火墙和路由器记录的安全事件；
6. 系统操作事件，包括系统启动和关闭，系统权限的创建、删除，设置或修改密

码；

7. 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 设施及陪同人和安全存储设施的访问；
8. 可信人员管理记录，包括网络权限的帐号申请记录，系统权限的申请、变更、创建申请记录，人员情况变化。

These events include but not limited to:

1. Management events in key's life cycle, including generation, backup, storage, recovery, usage, revocation, archiving, destruction, private key leakage, etc.
2. Management events in cryptography device's life cycle, including receiving, installation, uninstallation, activation, usage, repair, etc. for equipment.
3. The certificate application events, including the subscriber accept subscriber's agreement, the applied company, application data verification, application and validation data preservation, etc.
4. Management events of certificate life cycle, including application, approval, update, revocation, etc. System security events including: successful or unsuccessful access attempts for CA system, unauthorized access attempts for CA system network and files, operation (read, write or delete, etc.) for restricted and sensitive documents or records, system crash, hardware failures and other abnormal events.
5. Security events recorded via firewalls and routers.
6. System operating events, including startup and shutdown, creation or deletion of permission, configuration or modification of password.
7. Access to CA facilities, including the access of authorized or unauthorized personnel and attendants, and the access to security storage facilities.
8. Management record of trusted roles and personnel, including network account application, system permission application, modification, and creation, and the changes of personnel status.

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

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

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

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

GDCA 妥善保存电子认证服务的审计日志，在数据库保存审计日志至少两个月，保存期限为电子签名认证失效后十年。

GDCA saves electronic certification service audit logs properly. The retaining period of audit logs in database is at least two months. The preservation limitation period is ten years after the date of expiration of the electronic signature certification.

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

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

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

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

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

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

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

GDCA 设置自动审核系统以审核记录与资料，自动向有关人员或系统报告审核事件。

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 使用审计工具满足对上述系统审计的各项要求。

GDCA sets up an automatic validation system for audit records and data. It can report audit events to the relevant personnel or system automatically.

Audit log collection system involves in:

1) Certificate management system

2) Certificate issuing system

3) Certificate directory system

4) Remote communication system

5) Certificate accepted and approval system

6) Access and control systems

7) Security system of website, database

8) Other systems considered by GDCA for necessary audit.

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

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

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

GDCA 有权决定是否对导致事件的实体进行通告。

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

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

5.4.8. 脆弱性评估 Vulnerability Assessments

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

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

5.5. 记录归档 Records Archival

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

GDCA 对以下几类事件进行归档记录，包括但不限于：

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

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

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

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

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

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

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

1. Archiving for management events in subscriber certificate life cycle should be kept for more than 10 years.
2. Archiving for management events in CA Certificate and key life cycle should be kept for not less than life cycle of CA certificate and key.
3. Archiving retention period of subscriber certificates should not be less than 10 years after the expiration of certificates.
4. CA key and certificate archiving should be kept for 10 more years after the end of life cycle.

5.5.3. 归档文件的保护 Protection of Archive

GDCA 数据库由 GDCA 主密钥进行加密和保护。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。

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

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

对于系统生成的电子归档记录，每周进行备份，备份文件进行异地存放。

对于书面的归档资料，不需要进行备份，但需要采取严格的措施保证其安全性。

所有归档的电子文件和数据库除了保存在 GDCA 的存储库，还在异地保存其备份。

存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。GDCA 在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

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

For the written archiving data, they do not need to be backed up, but some strict measures need to be taken to ensure the security.

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

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

GDCA 的归档记录都标注时间，系统产生的记录按要求添加时间戳。

The archived records of GDCA are labeled with time, and the records generated by the system are required to be added a time stamp.

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

GDCA 的审计跟踪档案收集系统在本 CPS 第 5.4 节中作详细说明。

分离媒体数据存储和该媒体安全存储的归档不属于 GDCA 系统。

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

Storage of separated media data storage and archiving of its security storage are not included in GDCA system.

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

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

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

5.6. 电子认证服务机构密钥的更替 Key Changeover

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

1. 在下级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。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. GDCA 认证系统的口令由业务管理员、业务操作员、系统管理员进行变更。
2. 根据灾难的性质，部分或全部证书需要吊销或之后重新认证。
3. 如果目录无法使用或者目录有不纯的嫌疑，目录数据，加密证书和 CRL 需要进行恢复。
4. 及时访问安全现场尽可能合理地恢复操作。
5. 如果需要恢复业务管理员的配置文件，应由系统管理员执行恢复。
6. 如果需要恢复 GDCA 业务操作员的配置文件，则由另外一名 GDCA 安全业务操作员或业务管理员对其进行恢复。

In the intentional, man-made or natural disaster situation, GDCA will take the following steps to restore security environment:

1. GDCA verification system's password is changed by the business administrator, business operators and system administrator.
2. According to the type of disaster, some or all certificates should be revoked or re-verified later.
3. Directory data, encryption certificate and CRL are needed for recovery if the directory is unavailable or directory with impure suspicion.
4. Timely access to security site as far as possible to restore operation reasonably
5. While restore the business administrator's configuration file, it should be done by the system administrator.
6. While restore the GDCA business operator's configuration file, it should be done by another GDCA security business operator or administrator.

当 CA 根私钥被攻破、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。如果需要注销 CA 证书，将会采取以下措施：

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

5. GDCA 新的证书签发后，将立即通过 GDCA 信息库、目录服务器、HTTP 等方式发布。

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

1. GDCA reports immediately to the electronic authentication service management office and other government departments through the website and other public media to notify subscribers, and takes measures to protect user's interests without more losses.
2. GDCA notify the relevant parties to disconnect the systems associated with the certificate authentication services immediately.
3. GDCA revokes immediately all the certificates issued, and updates CRL and OCSP information for subscribers and relying parties. Meanwhile GDCA immediately generates a new key pair.
4. After the new root certificate has been issued, GDCA Re-issues the certificates and the subordinate CA certificate in accordance with the GDCA CPS about provisions of certificates issuing.
5. After the new root certificate has been issued by GDCA, it will be immediately published by GDCA repository, LDAP, HTTP, etc.

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

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

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

If private key of GDCA Subordinate CA is missing, tampering, cracking, leaking or used by unauthorized third parties suspiciously, Subordinate CA should:

1. Subordinate CA reports immediately to the GDCA and generates a new key pair and certificate request to apply for a new certificate.
2. GDCA reports immediately to the electronic authentication service management office and other government departments through the website and other public media to notify subscribers, and takes measures to protect user's interests without more losses.
3. GDCA notify the relevant relying party to close the system associated with the certificate authentication services immediately.
4. All the certificates issued by the Subordinate CA are revoked immediately to update information on CRL and OCSP for querying of certificate subscriber and relying party.
5. Subscriber certificate is re-issued in accordance with the CPS about provision of a certificate issued after the new Subordinate CA certificate has been issued.
6. After the new root certificate has been issued, it will be immediately published by the GDCA repository, LDAP, HTTP, etc. for distribution.

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

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

GDCA 在遭遇本节 5.8.1、5.8.2 和 5.8.3 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。

业务连续性的实施符合和 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 16 部分的要求。

在发生自然灾害或其他灾变，以致于无法在 24 小时内恢复证书状态服务时，将启用异地备份机房的设施，并于启用后 24 小时内恢复提供证书状态服务。

After encountering the disaster described in section 5.8.1, 5.8.2 and 5.8.3, GDCA can use the backup mechanisms to recover systems for operation and service delivery within 24 hours.

The enforcement of business continuity meets requirements of Section 16 guidelines published by CA/Browser Forum at www.cabforum.org.

If natural disasters or other catastrophes cause that certificate status service cannot be recovered within 24 hours, GDCA will use remote backup computer room facilities, and recover certificate status service within 24 hours.

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

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

在 GDCA 终止前，必须：

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

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

Before termination, GDCA must:

(1) Arrange the business to undertake

(2) Draft GDCA termination statement

(3) Notify the entities that are related to GDCA termination.

(4) Shut down subordinate LDAP

(5) Certificate revocation

(6) Treatment of archive file record

(7) Termination of certificate authority service.

(8) Archive main LDAP

(9) Shutdown main LDAP.

(10) Process GDCA business administrator and GDCA business operator.

(11) Process and store sensitive documents.

(12) Remove GDCA mainframe hardware

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

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

5.9. 数据安全 Data Security

数据安全符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 16 部分的要求。

Data security meets requirements of Section 16 guidelines published by CA/Browser Forum at www.cabforum.org.

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

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

6.1.1. 密钥对的生成 Key Pair Generation

CA 密钥对由国家密码主管部门批准和许可的设备生成的。密钥的生成、管理、存储、备份和恢复应遵循 FIPS140-2 标准的相关规定。由于 FIPS140-2 标准并非是国家密码主管部门认可和支持的标准，国家对于密码产品有严格的管理要求，因此 FIPS140-2 标准仅参照执行，是在国家密码管理政策许可前提下的选择性适用，具体参照设备厂商提供的资料。用于此类密钥生成的密码模块须通过国家密码主管部门鉴定、认证。

订户密钥对由订户自身的服务器或其它设备内置的密钥生成机制生成。GDCA 可接受为订户生成密钥对和 CSR，私钥加密保护后通过 SSL 加密连接传送给订户。订户密钥生成将由可信角色在使用了合适的随机数生成器或伪随机数生成器并满足或超过

FIPS 140-2 第二级别要求的加密设备中操作。密钥长度至少为 RSA 2048 位或 ECC 256 位。在 GDCA 网站使用私钥生成工具所产生的风险由订户承担。GDCA 不保存任何私钥和密码，所有这些信息在传送给用户后删除。

Key pair of CA is generated by the device approved and licensed by OSCCA. The generation, management, storage, backup and recovery of the key pair shall comply with the relevant regulations of FIPS140-2. Since FIPS140-2 is not a standard that approved and accepted by OSCCA and OSCCA implement a strict management of state's cryptographic products, GDCA only apply part of the provisions of FIPS140-2 under the permission of OSCCA. Specifically, the product manual of the device is for your reference. Hardware Security Module used for key generation must be evaluated and certified by OSCCA.

Subscriber's key pair is generated by the key generation mechanisms embedded in his/her own server or other devices. GDCA accepts the generation of keys and certificate signing requests for the subscribers, and the private keys are delivered encrypted and protected via SSL secured connection to the subscribers. Subscriber key generation is performed by personnel in trusted roles within a secure cryptographic device that uses a suitable random number generator (RNG) or pseudo random number generator (PRNG) and meets or exceeds the requirements of FIPS 140 level 2. The key sizes are at least RSA 2048 or ECC 256. The use of the private key generation utility at the GDCA website is at the sole risk of the subscriber. GDCA does not keep any private keys or passwords, and all such information is deleted after delivered to the subscribers.

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

私钥由订户自行生成，不需要将私钥传递给订户。GDCA 可接受为订户生成密钥对和 CSR，私钥加密保护后通过 SSL 加密连接传送给订户。

Subscriber's private key is generated by his/her own server or other devices. GDCA does not need to send private key to subscriber. GDCA accepts the generation of key pairs and certificate signing requests for the subscribers, and the private keys are delivered encrypted and protected via SSL secured connection to the subscriber.

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

最终订户和 RA 通过 PKCS#10 格式的证书签名请求信息或其它数字签名的文件包格式，以电子的方式将公钥提交给 GDCA 签发。

Subscriber and RA send request information, which contains public key, in digital form encoded as PKCS#10 or other packing format with digital signature to GDCA for issuing certificate.

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

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

Public keys of GDCA are included in the self-signed root CA certificate and business CA certificate, and published via GDCA's website. Subscribers and relying parties can transmit public keys by downloading them from this website.

6.1.5. 密码算法技术标准 Key Sizes

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

密钥长度符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 9.5 部分的要求。

The key size of RSA is at least 2048 bits. The key size of ECC is at least 256 bits.

The key size meets requirements of Section 9.5 guidelines published by CA/Browser Forum at www.cabforum.org.

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

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

对于参数质量的检查，同样由通过国家密码管理局批准许可的加密设备和硬件介质进行，例如加密机、加密卡、USB Key、IC 卡等。GDCA 认为这些设备和介质内置的协议、算法等已经具备了足够的安全等级要求。

Public key parameters must be generated in encryption equipment and hardware medium approved and permitted by State Cryptography Administration, such as encryption machine, encryption card, USB Key, IC card, and follow generation norms and standards of these devices. Of course, GDCA considers that built-in protocols, algorithms for these devices and medium have already met sufficient level of security requirements.

Quality of public key parameters is also checked through the encryption equipment and hardware

medium approved and permitted by State Cryptography Administration, such as encryption machine, encryption card, USB Key, IC cards. Of course, GDCA considers that built-in protocols, algorithms for these devices and medium have already met sufficient level of security requirements.

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

GDCA 签发的 X.509v3 证书包含了密钥用法扩展项，其用法与 RFC 5280 标准 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002) 相符。如果 GDCA 在其签发证书的密钥用法扩展项内指明了用途，证书订户必须按照该指明的用途使用密钥。

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

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

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

GDCA 所用的密码设备都是经国家密码管理局认可的产品。密钥的生成、管理、存储、备份和恢复应遵循 FIPS140-2 标准的相关规定。由于 FIPS140-2 标准并非是国家密码主管部门认可和支持的标准，国家对于密码产品有严格的管理要求，因此，GDCA 在选择加密设备时，仅参照 FIPS140-2 标准的要求，是在国家密码管理政策许可前提下的选择性适用，具体参照设备厂商提供的资料。用于此类密钥生成的密码模块须通过国家密码主管部门鉴定、认证。

Key pair of CA is generated by the device approved and licensed by OSCCA. The generation, management, storage, backup and recovery of the key pair shall comply with the relevant regulations of FIPS140-2. Since FIPS140-2 is not a standard that approved and accepted by OSCCA and OSCCA implement a strict management of state's cryptographic products, GDCA only refers to part of the provisions of FIPS140-2 under the permission of OSCCA. Specifically, the product manual of the device is for your reference. Hardware Security Module used for key generation must be evaluated and certified by OSCCA.

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

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

6.2.3. 私钥托管 Private Key Escrow

GDCA 的私钥不允许托管，也不向订户提供私钥托管服务。

GDCA does not escrow private key and doesn't provide the escrow service for subscriber.

6.2.4. 私钥备份 Private Key Backup

私钥备份分为三种类型的备份：初始化备份（当第一次安装系统后就需进行备份）、完全备份（定期对系统中私钥库制作拷贝）、增量备份（在系统进行大的改动后，应进行特别备份）。

初始化备份是系统初始化生成时进行的私钥备份。

完全备份是指私钥库的备份采用专门的备份软件进行完整备份，每周一次。增量备份是指私钥库的备份采用专门的备份软件进行增量备份，每天一次。

Private keys backup includes three types: initial backup (backup in the first installation), complete backup (regular copies of private key library in the system) and incremental backup (backup for big changes).

Initial backup is private key backup in the system installation.

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

6.2.5. 私钥归档 Private Key Archival

密钥管理中心对所生成的密钥信息进行归档保存，保存的方式为将密钥对分成三份分别用对称加密算法进行加密并保存在密钥管理中心的数据库中和磁盘阵列中。

密钥到期后，GDCA 在 10 天内完成归档操作。

Key management authority archives key information. It splits the key pair into three parts, encrypts them using symmetric encryption algorithm respectively, stores them in its database and disk.

Once the key reaches the expiration date, GDCA will complete the archiving operation in 10 days.

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

私钥信息是及其重要的信息，私钥信息的导出必须要导出到证书载体的密文存储区中。私钥信息的导出必须要将私钥信息进行三分，并对每部分的私钥信息进行对称加密才能存储到证书载体的存储区中，导入时必须三个证书载体同时导入，解密合并后才能导入。

Private keys are significant. The private key information must export to the cipher storage area of certificate carrier. The export of private key is as follows: GDCA must split the key into three parts, encrypt them using symmetric encryption algorithm respectively and store them in storage area of certificate carrier. The import of private key is as follows: GDCA must decrypt three parts described in export process, combine them into one and import the key.

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

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

用于安全存储 EV 代码签名证书订户私钥的硬件密码模块至少符合 FIPS 140-2 二级标准或同等级安全水平。

The private key of CA systems must be stored as cipher form in a Hardware Security Module approved and certified by OSCCA, and hardware cryptographic module at least meets the FIPS 140-2 level 3 standards or equivalent security levels.

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

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

CA 的私钥存放于硬件密码模块中，其激活数据按照 CPS 第 6.2.2 节进行分割，并且保存在 IC 卡等硬件介质中，必须由 3 名管理员同时在场，插入管理员卡并输入 PIN 码，才能激活私钥。

The private key of CA is stored in Hardware Security Module. Its activating data is split according to CPS section 6.2.2 and stored in IC card, etc. The method of activating private key is as follow: Three administrators are present at the same time and insert their cards and input their PIN codes.

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

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

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

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

如果私钥不再被使用，或者与私钥相对应的公钥到期或者被吊销后，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 the private key is no longer in use, or after the corresponding public key is expired or revoked, for the circumstance that the key is in software encryption module, it must be cleared by methods of mulching. For the circumstance that the key is in hardware encryption module, it should be cleared in the encryption device or IC card. Meanwhile, all the PIN codes, IC cards for activating private key also must be destroyed or recovered.

6.2.11. 密码模块的评估 Cryptographic Module Capabilities

GDCA 使用国家密码管理局批准和许可的密码产品。

GDCA uses the cryptogrammic products approved and permitted by OSCCA.

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

6.3.1. 公钥归档 Public Key Archival

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

密钥到期后，GDCA 在 10 天内完成归档操作。

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

Once the key reaches the expiration date, GDCA will complete the archiving operation in 10 days.

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

证书有效期符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 9.4 部分的要求相一致。

公钥和私钥的使用期限与证书的有效期相关，但并不完全保持一致。

对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期限以外。

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

The certificate validity period meets requirements of Section 9.4 guidelines published by CA/Browser Forum at www.cabforum.org.

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

For the signing certificate, its private key can only be used for signing within the certificate validity period and not be used beyond the validity period of certificate. However, in order to ensure signature information can be verified within the certificate validity period, the public key can be used beyond the validity period of certificate.

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

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

对于不同的证书，其密钥对允许通过证书更新的最长使用期限如下：

对于 RSA4096 位 CA 证书，其密钥对的最长允许使用年限是 30 年

对于 RSA2048 位 CA 证书，其密钥对的最长允许使用年限是 27 年

对于 ECC384 位 CA 证书，其密钥对的最长允许使用年限是 30 年

对于 ECC256 位 CA 证书，其密钥对的最长允许使用年限是 27 年

对于 RSA2048 位 EV 代码签名证书，其密钥对的最长允许使用年限是 39 个月

对于 RSA2048 位 EV SSL 服务器证书，其密钥对的最长允许使用年限是 825 天

对于 ECC256 位 EV SSL 服务器证书，其密钥对的最长允许使用年限是 825 天

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

For RSA 4096-bit CA certificate, the maximum usage period of the key pair is 30 years.

For RSA 2048-bit CA certificate, the maximum usage period of the key pair is 27 years.

For ECC 384-bit CA certificate, the maximum usage period of the key pair is 30 years.

For ECC 256-bit CA certificate, the maximum usage period of the key pair is 27 years.

For RSA 2048-bit EV CodeSigning certificate, the maximum usage period of the key pair is 39 months.

For RSA 2048-bit EV SSL server certificate, the maximum usage period of the key pair is 825 days.

For ECC 256-bit EV SSL server certificate, the maximum usage period of the key pair is 825 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

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

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

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

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

Activation data of CA private key must be generated, distributed and used strictly according to the requirements which are related to the segmentation of key activation data and key management. Activation data of subscriber private key, including password (provided in the form of password

envelope) used to download the certificate, USB Key, login password of IC card, must be generated randomly in secure and reliable environments.

Activation data generated by GDCA, including password (provided in the form of password envelope) used to download the certificate, USB Key, login password of IC card, must be generate randomly in secure and reliable environments. The activation data are delivered to subscribers safely and reliably, such as through offline face-to-face submission, post courier, delivery, etc. For activation data of non-single usage, GDCA suggests users to modify by themselves.

- 所有的保护口令都应该是不容易被猜到的
- 至少 12 位字符
- 至少包含一个数字和一个字母
- 不能包含很多相同的字符
- 不能和操作员的名字相同
- 不能使用生日、电话等数字
- 至少 90 天修改一次密码
- 不能与前四次的密码相同
- 每 90 天检查一次账户名和密码
- 移除 90 天内非活跃账户
- 证书系统登录尝试 5 次失败后即锁定账户
- All the protection passwords should not be guessed easily
- Contain at least twelve characters
- Contain one number and one letter at least
- Not contain many same characters
- Not be the same as operator’s name
- Not use birthdays, telephone numbers
- Modify the password in at least 90 days.
- Cannot be the same as the four passwords before.
- Check username and password every 90 days.
- Remove inactive account within 90 days.
- After failed 5 times login attempt of certificate system, the account is locked.

6.4.2. 激活数据的保护 Activation Data Protection

对于 CA 私钥的激活数据，必须将激活数据按照可靠的方式分割后由不同的可信人

员掌管，而且掌管人员必须符合职责分割的要求。

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

Activation data of CA private key must be separated in a reliable way and kept by different trusted personnel. Administrator must meet the requirements of responsibility division.

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

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

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

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

考虑到安全因素，对于申请证书的订户激活数据的生命周期，规定如下：

1、订户用于申请证书的口令，申请成功后失效。

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

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

The activation data of private key which is no longer used should be destroyed and protected from theft, disclosure or unauthorized use during the destruction. The result of destruction is that some or all of activation data can't be recovered directly or indirectly from the residual information and medium, papers recorded with passwords must be shredded.

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

1. The password used to apply for certificate becomes invalid after successful application.

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

6.5. 计算机安全控制 Computer Security Controls

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

GDCA 系统的信息安全管理，按照国标《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 ISO17799 信息安全标准规范以及其他相关的信息安全标准，制定出全面、完善的安全管理策略和制度，在运营中予以实施、审查和记录。主要的安全技术和控制措施包括：身份识别和验证、逻辑访问控制、物理访问控制、人员职责分权管理、网络访问控制等。

Information security management of GDCA certification system meets "Specifications Related Security Technology Certificate Authentication System" published by OSCCA; "Measures for the Administration of Electronic Certification Services" published by Ministry of Industry and Information Technology, standards of information security in ISO17799 and security standards of other relevant information. GDCA draws up comprehensive and perfect security management strategies and standards, which have been implemented, reviewed and recorded within operation. The main security technologies and control measures include: Identification and authentication, logic access control, physical access control, management of personnel's responsibilities decentralization, network access control, etc.

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

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

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

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

核心系统必须与其他系统物理分离，生产系统与其他系统逻辑隔离。这种分离可以阻止除指定的应用程序外对网络的访问。使用防火墙阻止从内网和外网入侵生产系统网络，限制访问生产系统的活动。只有 CA 系统操作与管理组中的、有必要工作需要、访

问系统的可信人员可以通过口令访问 CA 数据库。

系统安全符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 16.5 部分的要求。

Core system must be separated physically from other systems and the production system must be separated from other system logically. This separation can prohibit network access except for specific applications. The usage of firewall is to prevent the intrusion from the internal and external network production system and restrict activities of access production system. Only trusted persons in operation and management group of CA system, when necessary to access the system can access the CA database using password.

The system security meets requirements of Section 16.5 guidelines published by CA/Browser Forum at www.cabforum.org.

6.5.2. 计算机安全评估 Computer Security Rating

GDCA 根据法律法规和主管部门的规定，按照国家计算机安全等级的要求，实现安全等级制度。

GDCA 的认证系统，通过了国家密码管理局的安全性审查。

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

GDCA achieves a system of security level in accordance with the specifications of laws, regulations and administrative departments and the requirements of state computer security level.

GDCA certification systems pass the security review of OSCCA.

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

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

6.6.1. 系统开发控制 System Development Controls

GDCA 的软件设计和开发过程遵循以下原则：

1. 制定公司内部的升级变更申请制度，并要求工作人员严格按照流程执行；
2. 制定公司内部的采购流程及管理制度；
3. 开发程序必须在开发环境进行严格测试成功后，再申请部署于生产环境；

4. 变更部署前进行有效的在线备份；
5. 第三方验证和审查；
6. 安全风险分析和可靠性设计；

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

Software design and development of GDCA process follows principles:

1. Establish internal system of corporation about update, alteration and application. The employees should follow this system strictly.
2. Establish internal purchasing process and management system of corporation.
3. After the programs have passed strict test in development environment, they can be deployed to production environment.
4. Effective online backup must be done before deployment changes.
5. Verification and review of third-party
6. The security risk analysis and reliability design

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

6.6.2. 安全管理控制 Security Management Controls

GDCA 认证系统的信息安全管理，严格遵循国家密码管理局的有关运行管理规范进行操作。

GDCA 认证系统的使用具有严格的控制措施，所有的系统都经过严格的测试验证后才进行安全和使用，任何修改和升级会记录在案并进行版本控制、功能测试和记录。GDCA 还对认证系统进行定期和不定期的检查和测试。

GDCA 采用一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。

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。

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

GDCA authentication system has strict control measures, and all the systems can be used only

after being rigorously tested and verified. .Any modifications and upgrades will be recorded for reference and made for version control, functional test and record. GDCA also carries out regular and irregular inspection and test on certification system.

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

Hardware devices are checked from the perspective of intrusion and security holes, etc. Encryption devices must be examined, installed and accepted in a strict security control mechanism.

After all the hardware and software equipment of GDCA authentication system are upgraded, GDCA must confirm the existence of information which affects the security in waste equipment.

6.6.3. 生命周期的安全控制 Life Cycle Security Controls

GDCA 认证系统的软硬件设备具备可持续性的升级计划，其中包括了对软、硬件生命周期的安排。

Software and hardware of GDCA certification system have sustainable upgrade plan such as arrangement of software and hardware lifetimes.

6.7. 网络的安全控制 Network Security Controls

GDCA 认证系统采用多级防火墙和网络资源安全控制系统的保护，并且实施完善的访问控制技术。

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

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

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

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

In order to ensure network security, GDCA authentication business system has been equipped with intrusion detection, security auditing, virus protection and network management systems, and updated to the version of above systems, as much as possible to reduce the risks from the network.

6.8. 时间戳 Time-Stamping

认证系统的各种系统日志、操作日志都应该有相应的时间标识。这些时间标识不需要采用基于密码的数字时间戳技术。

All kinds of system log and operation log of authentication system should contain a corresponding time records. The time records do not need to use the technology of digital time-stamping based on encryption.

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

7.1. 证书 Certificate Profile

GDCA 证书遵循 ITU-T X.509v3（1997）：信息技术-开放系统互连-目录：认证框架（1997 年 6 月）标准和 RFC 5280：Internet X.509 公钥基础设施证书和 CRL 结构（1999 年 1 月）。

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

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

GDCA certificate format is in accordance with ITU-T X.509 V3 (1997): information technology -- open systems interconnection -- the directory: authentication framework (June 1997) standard and RFC 5280: Internet X.509 public key infrastructure certificate and CRL structure (Jan1999).

EV certificate contains at least X.509 V1 domain, its specified values or value restrictions are as the following table described.

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

表-EV 证书结构的基本域

域	值或值的限制
版本	指明 X.509 证书的格式版本，值为 V3
序列号	证书的唯一标识符
签名算法	签发证书时所使用的签名算法（见 CPS 第 7.1.3 节）
签发者 DN	签发者的甄别名
有效起始日期	基于国际通用时间(UTC)，和北京时间同步，按 RFC 5280 要求编码

有效终止日期	基于国际通用时间(UTC)，和北京时间同步，按 RFC 5280 要求编码。有效期限的设置符合本 CPS 规定的限制。
主题 DN	证书持有者或实体的甄别名
公钥	根据 RFC 5280 编码，使用 CPS 中指定的算法，密钥长度满足 CPS 指定的要求

Basic domain of EV Certificate structure

domain	Value or value limitation
Version	Format version of X.509 certificate，the value is V3
Serial number	Unique identifier of certificate
Signature algorithm	Signature algorithm for issuing certificate（see CPS section 7.1.3）
Issuer DN	Issuer's Distinguish Name
Start period	Based on the Coordinated Universal Time (UTC), Synchronized with Beijing time, encoding follows the requirements of RFC 5280.
End period	Based on the Coordinated Universal Time (UTC),Synchronized with Beijing time, encoding follows the requirements of RFC 5280. The setting of valid period follows the limitation of this CPS specified.
Subject DN	DN of certificate holder or entity
Public key	Using algorithm specified in this CPS and according to the encode of RFC 5280，key size meets specified requirements of this CPS.

7.1.1. 版本 Version Number(s)

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

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

7.1.2. 证书扩展项 Certificate Extensions

GDCA 除了使用 X.509 V3 版证书标准项和标准扩展项以外，还使用了自定义扩展项，证书扩展项遵循 IETF RFC 5280 标准，并符合 Guidelines For The Issuance And Management Of Extended Validation Certificates 的要求。

1. 证书标准项

- 证书版本号(Version)

指明 X.509 证书的格式版本，值为 V3。

- 证书序列号（SerialNumber）

即由 GDCA 分配给证书的唯一的数字型标识符。

- 签名算法标识符（Signature）

指定由 GDCA 签发证书时所使用的签名算法。

- 签发机构名（Issuer）

用来标识签发证书的 CA 的 X.500 DN 名字。即 GDCA 各个属性，包括国家、省、市、机构、单位部门、和通用名。

CN = GDCA Guangdong Certificate Authority

OU = Guangdong Certificate Authority

O = GDCA Certificate Authority

L = Guangzhou

S = Guangdong

C = CN

- 证书有效期（Validity）

用来指定证书的有效期，包括证书开始生效的日期和时间以及失效的日期和时间。每次使用证书时，需要检查证书是否在有效期内。

- 证书用户名（Subject）

指定证书持有者的 X.500 唯一名字。包括国家、省、市、机构、单位部门和通用名，还可包含 email 地址等个人信息等。

- 证书持有者公开密钥信息（subjectPublicKeyInfo）

证书持有者公开密钥信息域包含两个重要信息：证书持有者的公开密钥的值；公开密钥使用的算法标识符。此标识符包含公开密钥算法和 hash 算法。

In addition to the X.509 V3certificate standard items and standard extension items, GDCA also uses customized extensions. The certificate extensions follow the IETF RFC 5280 standard, and conform to the requirements of the Guidelines for The Issuance And Management Of Extended Validation Certificates.

1. certificate standard items

- Version

This field describes the version of X.509 certificate.

- Serial Number

The serial number is a unique integer assigned by GDCA to each certificate.

- Signature Algorithm Identifier

The algorithm identifier is used to identify a signing algorithm with which GDCA used to Issuer.

- Issuer

The issuer field identifies X.500 DN of CA that has signed and issued the certificate, namely each attribute of GDCA, including country, province, city, organization, department and common name.

CN = GDCA Guangdong Certificate Authority

OU = Guangdong Certificate Authority

O = GDCA Certificate Authority

L = Guangzhou

S = Guangdong

C = CN

- Validity

The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate, including two dates: the date on which the certificate validity period begins and the date on which the certificate validity period ends. The validity must be checked each time using certificates.

- Subject

The subject field identifies X.500 DN of subscriber, including country, province, city, organization, department and common name. It may also contain email addresses and other personal information.

- Subject Public Key Info

This field is used to carry the public key and identify the algorithm with which the key is used. This identifier identifies public key algorithm and hash algorithm.

2. 证书扩展项

- 颁发机构密钥标识符（Issuer Unique Identifier）

此域用在当同一个 X.500 名字用于多个认证机构时，用一比特字符串来唯一标识签发者的 X.500 名字。

- 主题密钥标识符（Subject Unique Identifier）

此域用在当同一个 X.500 名字用于多个证书持有者时，用一比特字符串来唯一标识证书持有者的 X.500 名字。

- 密钥用法 (key usage)

指定各种密钥的用法：电子签名，不可抵赖，密钥加密，数据加密，密钥协议，验证证书签名，验证 CRL 签名，只加密，只解密，只签名。

- CRL 发布点

由 GDCA 指定的 CRL 发布点。

2. Certificate extensions

- Authority Key Identifier

The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. This extension is used where an issuer has multiple signing keys (either due to multiple concurrent key pairs or due to changeover).

- Subject Key Identifier

The subject key identifier extension provides a means of identifying certificates that contain a particular public key. The extension identifies the authorized public key. It provides a means to identify different keys used by the same subject (e.g. when rekeying).

- Key usage

The key usage extension defines the purpose (e.g., electronic signature, non-repudiation, key encryption, data encryption, key protocol, certificate signature verification, CRL signature validation, only encryption, only decryption and only signature) of the key contained in the certificate.

- CRL Distribution Points

It refers to CRL Distribution Points specified by GDCA.

3. 自定义扩展项

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

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

3. Customized extensions

To satisfy different requirements for certificate application service, GDCA can define some extensions flexibly, including but not limited to the following extensions:

- Insurance number: It is used to indicate the subscriber's insurance number.
- Organization Code: It is used to indicate the Organization code.
- IC registration number: It is used to indicate enterprise IC registration number.

- Taxation registration certificate number: It is used to indicate enterprise national taxation number.
- Trusted service number: It is used to indicate subscriber's unique number generated by GDCA.
- Land taxation registration certificate number: It is used to indicate enterprise land taxation number.
- Resident identity card number: It is used to indicate unique number of resident's identity card.

7.1.3. 算法对象标识符 Algorithm Object Identifiers

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

The signing algorithm identifier of certificate issued by GDCA is sha256RSA and sha256ECDSA.

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。

Name of certificate issued by GDCA is formatted in accordance with X.501 DN.

7.1.5. 名称限制 Name Constraints

无规定。

No stipulation.

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

GDCA 签发的 EV 证书应包含证书策略的对象标识符。

证书标识符符合 CA/浏览器论坛（CA/Browser Forum）通过 www.cabforum.org 发布的指南 9.3 部分的要求。

EV certificate issued by GDCA shall contain certificate policy object identifier.

Certificate policy object identifier meets requirements of Section 9.3 guidelines published by CA/Browser Forum at www.cabforum.org.

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

不适用。

No provisions.

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

不适用。

No provisions.

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

与 X509 和 PKIX 规定一致。

Conform to X509 and PKIX.

7.2. 证书吊销列表 CRL Profile

GDCA 定期签发 CRL，供用户查询使用。

GDCA issues CRL regularly for the subscribers to query.

7.2.1. 版本 Version Number(s)

GDCA 的证书吊销列表采用 X.509 v2 版的证书格式。

CRL issued by GDCA is formatted in accordance withX.509 V2.

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

GDCA 的证书吊销列表（CRL）是一个带有时间戳并且经过数字签名的已吊销证书的列表。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。

- 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。
- 签名算法：GDCA 采用 sha256RSA 和 sha256ECDSA 签名算法。

- 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。
- 生效时间：指定一个日期/时间值，用以表明本 CRL 发布的时间。
- 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）。
- 吊销证书列表：指定已经吊销的证书列表。本列表中含有证书的序列号和证书被吊销的日期和时间。
- 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。

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.

- CRL version: It refers to version information of CRL, GDCA adopts CRL V2 corresponding to X.509 V3 certificate.
- Signature algorithm: GDCA adopts sha1 RSA,sha256RSA, sha256ECDSA, SM2 and ECC signature algorithms.
- Issuer: It refers to DN of issuing authority, including country, province, city, organization, department and common name, etc.
- Effective time: It refers to date/time which indicates CRL issuing time.
- Update time: It refers to date/time which indicates next issuing time of CRL. (It's an enforced field in this CPS).
- Certificate Revocation List: It refers to a list of revoked certificates. The list contains certificate serial number and certificate revocation date and time.
- 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.

7.3. 在线证书状态协议 OCSP Profile

GDCA 采用 IETF PKIX 工作组开发的一个在线证书状态协议 (Online Certificate Status Protocol，OCSP，RFC6960)，该协议定义了一种标准的请求和响应信息格式以确认证书是否被撤销了。在 GDCA 官方网站下载 OCSP 查询客户端并按照 GDCA 官方网站发布的 OCSP 操作说明进行配置，即可使用 GDCA 的在线证书状态查询服务。GDCA 签发的 OCSP 响应至少包含以下所述的 OCSP 机构基本域和内容：

- Version：客户端使用的 OCSP 协议的版本号；GDCA 的在线证书状态协议为 v1 版。

- signatureAlgorithm：签发 OCSP 的算法；
- responderID：签发 OCSP 的实体。签发者公钥的 SHA1 数据摘要值和证书甄别名。
- producedAt：OCSP 响应生成的日期和时间；
- Signature：OCSP 响应消息的数字签名。
- Nonce(一次性随机数)：在状态请求消息中的每一个 requestExtensions 变量和响应消息中的 responseExtension 变量中包含一次性随机数，防止重放攻击。
- 证书状态：证书的最新状态，包括有效、吊销和未知。

GDCA adopts an Online Certificate Status Protocol (OCSP, RFC6960) developed by IETF PKIX working group. This protocol defines a standard request and response information formats to query whether a certificate is revoked. Subscribers can download the OCSP query client from GDCA official website and follow the OCSP guide book published at GDCA official website for configuration. Then subscribers can use GDCA's online certificate status query service. OCSP response message issued by GDCA contains at least OCSP organization basic domains and contents described below:

- Version: OCSP protocol version number used by client. The version of GDCAOCSP is v1.
- SignatureAlgorithm: Algorithm used for signing and issuing OCSP.
- ResponderID: ID of entity who issues OCSP. It consists of SHA1 of issuer’s public key and DN of certificate.
- ProducedAt: Date and time when OCSP response message is generated.
- Signature: Digital signature of OCSP response message
- Nonce: The nonce, which is used to prevent replay attacks, is included in requestExtensions variable of state request message and responseExtension of response message.
- Certificate status: The latest status of certificate, including effective, revocation and unknown.

7.3.1. 版本号 Version Number(s)

RFC2560 定义的 OCSP V1 版本。

The field conforms to OCSP V1 defined in RFC2560.

7.3.2. OCSP 扩展项 OCSP Extensions

无规定。

No provisions.

7.3.3. OCSP 请求和响应处理 Processing of OCSP Request and Response

一个 OCSP 请求包含以下数据：协议版本、服务要求、目标证书标识和可选的扩展项等。

在接受一个请求之后，OCSP 服务端响应时进行如下检测：

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

An OCSP request contains the following data: Protocol version, service request, target certificate identifier and optional extensions, etc.

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

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

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

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

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

- Reply syntax version
- Response server name
- Response to the request client certificate
- Optional extensions
- Signature Algorithm object identifier

- The signature after the response information is hashed

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

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

If an error occurs, OCSP server will return an error message, which doesn't contain key signature signed of GDCA certificate issuer. The error message includes:

- malformedRequest
- internalError
- trylater
- sigRequired
- unauthorized

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 and Circumstances of Assessment

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

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

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

2、GDCA 按照国家主管部门的要求、国家相关标准和本 CPS 的规定实施运营和服务，按照内部评估和审计规范，每年至少定期执行一次内部的评估审核，包括对 GDCA 内其它实体（RA、受理点等）的评估审核。

3、GDCA 聘请独立的审计师事务所，按照 WebTrust 对 CA 的审计规则，每年进行一次外部审计和评估。

4、GDCA 每年进行一次风险评估工作，识别内部与外部的威胁，评估威胁事件发生的可能性及造成的损害，并评估目前的应对策略、技术、系统以及相关措施是否足够应对风险，根据风险评估，创建、实施并维持涵盖安全流程、措施及产品的安全计划。

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

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

In addition to internal audits and assessments, GDCA also engages external audit firms to perform assessments and evaluations according to the CA requirements of WebTrust on CA.

1. GDCA is assessed and inspected once a year in accordance with the "Electronic Signature Law of the People's Republic of China", "Measures for the Administration of Electronic Certification Services" and other requirements by administrative authorities.
2. GDCA conducts operations and services according to the requirements of state’s authorities, the specifications of state’s relevant standards and this CPS. GDCA should conduct internal assessment and audit to other entities (including RA or LRA, etc.) in GDCA at least once a year.
3. GDCA engages external audit firms to conduct assessments and evaluations once a year to be compliant with WebTrust for CA.
4. GDCA performs a risk assessment once a year to identify internal and external threats, and to evaluate the possibility of occurrence and potential damages, and to assess if the current strategies, technologies, systems and relevant measures are able to mitigate these risks. Based on the risk assessment, GDCA develops, implements, and maintains a security plan consisting of security procedures, measures, and products.

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

8.2. 评估者的资质 Identity/Qualifications of Assessor

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

GDCA 聘请的外部审计机构，应该具备以下的资质：

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

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

External auditors which GDCA hires should have the following qualifications:

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

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

1、 GDCA 审计员与本机构的系统管理员、业务管理员、业务操作员的工作岗位不能重叠。

2、 外部评估者(信息产业主管部门、独立审计师事务所以及其他机构)和 GDCA 之间是独立的关系，没有任何的业务、财务往来，或者其它任何利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对 GDCA 进行评估。

1、 Segregation of duties is required between the GDCA auditors, and the GDCA system administrators, business administrators, and business operators.

2、 The external evaluators (information industry department, independent audit firms and other authorities) and GDCA are independent from each other. There is no business interaction, financial transactions, or any other interests that could affect the objectivity of the assessment between the above two. Assessors should evaluate GDCA in an independent, fair and unbiased attitude.

8.4. 评估内容 Topics Covered by Assessment

GDCA 中心的审计工作包括以下内容：

1、 安全策略是否得到充分的实施；

2、 运营工作流程和制度是否得到严格遵守；

3、 是否严格按 CPS、业务规范和安全要求开展认证业务；

4、 各种日志、记录是否完整，是否存在问题；

5、 是否存在其他可能存在的安全风险。

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

GDCA's audit contents include:

1、 Whether the security strategy is fully implemented

2、 Whether operation procedures and processes strictly followed

3、 Whether strictly following the CPS, business specifications and security requirements when conducting authentication services

4、 Whether all kinds of logs and records are preserved and if there is any question

5、 If there's any other potential security risks

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

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

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

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

第三方审计师事务所评估完成后，GDCA 按照其工作报告进行整改，并接受再次审计和评估。

Audit assessment group monitors responsible departments for improvements and complete status

of issues that were mentioned in audit reports. After improvement of audit results have completed, various functional departments should submit summary of improvement to audit assessment group.

For authorized RA mentioned in GDCA's audit report, if they are violating the CPS and other business standards defined by GDCA, GDCA will stop the above behaviors immediately and ask them to make changes in accordance with the requirements of GDCA.GDCA will terminate relevant authorization of electronic certification services of RA if the above behaviors are seriously violated.

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

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

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

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

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

If the assessment from a third-party auditor firm is completed, the audit results will be published at GDCA website (www.gdca.com.cn). Third-party should communicate its purposes and methods to GDCA in advance before notifying the evaluation entity on the assessment results or similar information, except otherwise defined by law; GDCA reserves the legal rights in this part.

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 or 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，具体收费标准根据行业市场收费情况而定。在收费标准范围内，即不超过收费标准的情况下，GDCA 有权根据市场状况，针对不同订户群体推出不同的收费策略或优惠措施。

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

GDCA can charge subscriber certification fees for the digital authentication service provided. The specific charge standards are executed according to the approved documents of state related price administration department. In the standard range of the charge, namely not exceeding the upper limit, GDCA has the rights to launch different charging and discount policies targeted to different subscriber groups.

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

9.1.2. 证书查询费用 Certificate Access Fees

在证书有效期内，对该证书信息进行查询，目前 GDCA 不收取查询费用。除非用户提出的特殊需求，需要 GDCA 支付额外的费用，GDCA 将与用户协商收取应该收取的费用。

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

Currently, GDCA doesn't charge for inquiry during the certificate validation period. Unless the subscriber has special requests, which makes GDCA to pay extra fees, GDCA will interact with the subscriber for appropriate charges.

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

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

GDCA 对于证书吊销和状态查询，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。

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

GDCA currently does not charge any fees for the certificate revocation and status inquiry. Unless the subscriber has special requests, which makes GDCA to pay extra fees, GDCA will interact with the subscriber for appropriate charges.

If revocation and status information inquiry charging policy has any changes, GDCA will promptly post the changes at its website (www.gdca.com.cn).

9.1.4. 其他服务费用 Fees for Other Services

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

2、 GDCA 将向用户提供证书存储介质及相关服务，GDCA 在与订户或者其他实体签署的协议中指明该项价格。

3、 其他 GDCA 将要或者可能提供的服务的费用，GDCA 将会及时公布，供用户查询。

1、 If subscriber requests paper version of CPS or other related documents from GDCA, GDCA will charge postage and processing fees.

2、 GDCA provides certificate storage media and related services to subscribers. GDCA declares the prices of above items in the agreements signed with subscribers or other entities.

3、 Other services fees that GDCA may or will charge will be published timely for referencing.

9.1.5. 退款策略 Refund Policy

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

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

此退款策略不限制订户得到其它的赔偿。

完成退款后，订户如果继续使用该证书，GDCA 将追究其法律责任。

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

In the process of the certificate operation and the certificate issuance, GDCA complies with strict operating procedures and policies. If GDCA violates its defined responsibilities under this CPS or other material obligations, subscribers can request GDCA to revoke certificates and refund. After GDCA revokes subscriber's certificates, GDCA will immediately refund the full amount that subscribers have paid for the certificate application.

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

After refund completion, if a subscriber continues to use the certificate, GDCA shall investigate his/her legal liabilities.

9.2. 财务责任 Financial Responsibility

9.2.1. 保险范围 Insurance Coverage

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

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

证书类型	赔偿金额上限
EV 代码签名证书	300000 元（RMB）
EV SSL 服务器证书	1000000 元（RMB）

If the following circumstances occur and is confirmed by GDCA, certificate subscribers, relying parties and other entities can request GDCA assume compensation liabilities (except for statutory or contractual exemptions).

- GDCA issues certificates to a third-party instead of the subscriber by mistake, which leads to losses of the subscriber or relying party.
- After GDCA knows the fact that subscriber provides fake registration information or data, GDCA still issues certificate, which leads to relying party suffering losses.
- GDCA issues certificates without authenticating subscribers' application and it leads to the losses of subscribers or relying party.
- If the private key of the certificate is deciphered or stolen due to the fault of GDCA, which leads to the subscriber or relying party suffering losses.
- GDCA fails to revoke the certificate in time.
- The maximum compensation amount for the certificate is as follow:

Type	Maximum Compensation Amount
EV code signing certificates	300000 (RMB)
EV SSL server certificates	1000000(RMB)

9.2.2. 其他财产 Other Assets

不适用。

No stipulation.

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

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

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

2、 GDCA 只有在证书有效期限内承担损失赔偿责任。

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

1、 All the compensation obligation of GDCA shall not exceed the insurance coverage stipulated in section 9.2.1.The amount of compensation shall not be higher than the compensation maximum amount. GDCA can reset the compensation maximum amount. GDCA will notify relevant parties immediately after the reset.

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

9.2.4. 责任免除 Liability Exemption

1、 有下列情形之一的，应当免除 GDCA 之责任：

1) 订户在申请和使用 GDCA 数字证书时，有违反如下义务之一的：

2) 订户有义务提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信

息；

3) 订户应当妥善保管 GDCA 所签发的数字证书载体和保护 PIN 码，不得泄漏 PIN 码或将数字证书载体随意交付他人；

4) 订户在应用自己的密钥或使用数字证书时，应当使用可依赖、安全的系统；

5) 订户知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知 GDCA 及相关各方，并终止使用该电子签名制作数据；

6) 订户在使用数字证书时必须遵守国家的法律、法规和行政规章制度。不得将数字证书作为 GDCA 规定使用范围外的其他任何用途使用；

7) 订户必须在证书有效安全期内使用该证书；不得使用已失密或可能失密、已过有效期、被冻结、被吊销的数字证书；

8) 订户有义务根据规定按时向 GDCA 及当地业务受理点交纳服务费用。

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

1) If one of the following obligations are violated when subscribers are applying and using GDCA digital certificates:

2) The subscriber has the obligation to provide real, complete, accurate material and information, and forbid to provide fake, invalid materials and information;

3) The subscriber shall properly keep the certificate carrier issued by GDCA and protect PIN code, and forbid to leak the PIN code or deliver the certificate carrier to others at discretion;

4) When the subscribers are using their own keys or certificates, they shall use reliable and secure systems.

5) If the subscriber has known data used for making electronic signature (private key) has been compromised or may have been compromised, he/she should inform GDCA and related parties promptly, and terminate the use of data used for making electronic signature;

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

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

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

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

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

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

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

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

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

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

1) 不可抗力；

2) 关联单位如电力、电信、通讯部门而致；

3) 黑客攻击；

4) GDCA 的设备或网络故障。

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

1) Force majeure

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

3) Hacker attacks

4) Equipment or network failure of GDCA

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

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

9.3. 业务信息保密 Confidentiality of Business Information

9.3.1. 保密信息范围 Scope of Confidential Information

在 GDCA 提供的电子认证服务中，以下信息视为保密信息：

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

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

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

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

GDCA 将以下信息视为不保密信息：

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

GDCA treats the following information as non-confidential information:

- Information in the certificate and CRL issued by GDCA
- Information in certificate policy supported by GDCA and recognized by CPS
- Information that is permitted by GDCA, only used by GDCA subscribers and published at the

GDCA website

- Others: The confidentiality of GDCA information depends on particular data items and applications

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

GDCA 有妥善保管与保护本节 9.3.1 中规定的保密信息的责任与义务。

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

9.4. 个人隐私保密 Privacy of Personal Information

9.4.1. 隐私保密方案 Privacy Plan

GDCA 尊重证书订户个人资料的隐私权，保证完全遵照国家对个人资料隐私保护的相关规定及法律。同时，GDCA 将确保全体职员严格遵从安全和保密标准对个人隐私给予保密。

GDCA respects the privacy of the certificate subscriber's personal data and guarantees to fully comply with the relevant national laws and regulations. In the meantime, GDCA requires all employees strictly comply with security and confidential standards for personal privacy.

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

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。

GDCA defines the following information as certificate subscriber's privacy information:

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

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

GDCA 定义包括但不限于以下信息不被视为证书订户的隐私信息：

- 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。

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

- Subscriber’s name, organization name
- Subscriber’s gender, organization nature
- Subscriber’s postal code of mailing address
- Subscriber’s email address

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9.5. 知识产权 Intellectual Property Rights

- GDCA 享有并保留对证书以及 GDCA 提供的所有软件的全部知识产权。
- GDCA 对数字证书系统软件具有所有权、名称权、利益分享权。
- GDCA 有权决定采用何种软件系统。
- GDCA 网站上公布的一切信息均为 GDCA 财产，未经 GDCA 书面允许，他人不能转载用于商业行为。
- GDCA 发行的证书和 CRL 均为受 GDCA 支配的财产。

- 对外运营管理策略和规范为 GDCA 财产。
- 用来表示目录中 GDCA 域中的实体的甄别名（以下简称 DN）以及该域中颁发给终端实体的证书，均为 GDCA 的财产。
- GDCA reserves and remains full intellectual property rights for all the certificates and software offered by GDCA.
- GDCA holds ownership, the right of name, the right to share the benefits for certificate system software.
- GDCA has the right to decide to use which software system.
- All the information published at GDCA website is GDCA property. Without written permission of GDCA, others cannot repost them for commercial activities.
- Certificates and CRLs issued by GDCA are both the properties controlled by GDCA.
- External operation management strategy and specification are GDCA properties.
- The distinguished name (hereinafter referred to as DN) used to express the GDCA domain entity in the directory and the certificate issued to the terminal in the domain entity are the properties of GDCA.

9.6. 陈述与担保 Representations and Warranties

9.6.1. 电子认证服务机构的陈述与担保 CA Representations and Warranties

GDCA 在提供电子认证服务活动过程中对订户的承诺如下：

- 签发给订户的证书符合 GDCA 的 CPS 的所有实质性要求。
- 将向证书订户通报任何已知的，将在本质上影响订户的证书的有效性和可靠性事件。
- 将根据 CPS 的要求及时吊销证书。
- 拒绝签发证书后，将立即向证书申请者归还所付的全部费用。
- 验证申请者对列在证书主题字段及主题别名扩展（或，仅针对域名而言，获得了拥有域名使用权或控制权人士的授权）中的域名及 IP 地址拥有使用权或控制权；
- 验证申请者授权了证书的签发以及申请者代表获得了授权，以代表申请者申请证书；
- 验证证书中所包含的全部信息的准确性（organizationalUnitName 信息除外）；
- 采取验证措施以减小证书主题“organizationalUnitName”中所包含的信息存在

误导的可能性；

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

证书公开发布后，GDCA 保证除未经验证的订户信息外，证书中的其他订户信息都是准确的。

GDCA 不负责评估证书是否在适当的范围内使用，订户和依赖方依照订户协议和依赖方协议确保证书用于允许使用的目的。

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

- Certificates issued to subscribers by GDCA must be in line with all substantive requirements of this CPS.
- Informs subscribers any known events, which will fundamentally affect the validity and reliability of the certificate.
- Revokes the certificate acoording to this CPS.
- After refusing to issue a certificate, GDCA would immediately refund the fee that the applicant has paid for the certificate.
- Verifies that the applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control);
- Verifies that the applicant authorized the issuance of the certificate and that the applicant representative is authorized to request the certificate on behalf of the applicant;
- Verifies the accuracy of all of the information contained in the certificate(with the exception of the organizationalUnitName information);
- Implements a procedure for reducing the likelihood that the information contained in the certificate's subject: organizationalUnitName attribute would be misleading;
- Verifies the identity of the applicant according to section 3.2 of this CPS;
- Subscriber agreement: That, if GDCA and subscribers are not affiliated, the subscriber and GDCA are parties to a legally valid and enforceable subscriber agreement that satisfies the Baseline Requirements and other requirements published by the CA/Browser Forum, or, if GDCA and subscribers are the same entity or are affiliated, the applicant representative

acknowledged the terms of use;

- Maintains a 24 x 7 publicly-accessible repository with current information regarding the status (valid or revoked) of all unexpired certificates;

After the certificate has issued to the public, GDCA guarantees that the subscriber information in the certificate are accurate except the unauthenticated subscriber information.

GDCA is not responsible for the assessment of whether a certificate is used within an appropriate scope. Subscriber and relying party ensure the certificate is used for appropriate purposes based on the subscriber agreements and relying party agreements.

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：

- 提供给证书订户的注册过程完全符合 GDCA 的 CPS 的所有实质性要求。
- 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。
- 注册机构将按 CPS 的规定，及时向 GDCA 提交吊销、更新等服务申请。

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

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

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

订户一旦接受 GDCA 签发的证书，就被视为向 GDCA、注册机构及信赖证书的有关当事人作出以下承诺：

- 已知悉和接受 GDCA 的“数字证书申请责任书”和本 CPS 中的所有条款和条件。
- 在证书的有效期内进行数字签名。
- 订户在申请证书时向注册机构提供的信息都是真实、完整和准确的，愿意承担任何提供虚假、伪造等信息的法律责任。
- 如果存在代理人，那么订户和代理人两者负有连带责任。订户有责任就代理人

所作的任何不实陈述与遗漏，通知 GDCA 或其授权的证书服务机构。

- 与订户证书所含公钥相对应的私钥所进行的每一次签名，都是订户自己的签名，并且在进行签名时，证书是有效证书（证书没有过期、吊销），证书的私钥为订户本身访问和使用。
- 除非经订户和发证机构间书面协议明确规定，订户保证不从事发证机构（或类似机构）所从事的业务。
- 一经接受证书，即表示订户知悉和接受本 CPS 中的所有条款和条件，并知悉和接受相应的订户协议；
- 一经接受证书，订户就应当承当如下责任：始终保持对其私钥的控制，使用可信的系统，采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用；
- 不得拒绝任何来自 GDCA 公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等；
- 证书在本 CPS 中规定使用范围内合法使用，只将证书用于经过授权的或其他合法的使用目的；
- 采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件；
- 对于 EV SSL 证书，订户有责任和义务保证只在证书中列出的主题别名对应的服务器中部署证书。
- 对于 EV 代码签名证书的订户，若发现以下情况，应立即向 GDCA 申请吊销证书：1）证书中的信息为或将成为错误或不准确的信息；2）证书中与公钥有关的私钥被误用或被损坏；3）有证据表明，该代码签名证书被用于签署可疑代码。

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

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

- Each signature is generated using the private key corresponding to certificate by subscribers themselves. The certificates shall be valid at the moment of signing, i.e. certificate is not revoked or expired.
- Subscribers ensure that they don't engage in business performed by the issuing agency (or similar institutions) unless they sign written agreements with the issuing agency on such matters.
- Once the certificate is accepted, subscribers are considered as knowing and accepting all the terms and conditions in the CPS as well as corresponding subscriber agreements.
- Once the certificate is accepted, the subscriber should assume the following responsibilities: always maintain control of their private keys; use trustworthy systems; and take reasonable precautions to prevent the loss, disclosure, alteration, or unauthorized usage of the private keys.
- Prohibited for rejecting any statements, changes, updates and upgrades published by GDCA, including but not limited to modification of strategies and standards as well as additions and deletions of certificate services.
- The subscriber only uses certificate for the authorized or other lawful purpose within the range specified by this CPS.
- The subscriber use secure and reasonable measures to prevent the private key from loss, disclosure, alteration and other events.
- For the EV SSL certificates, the subscribers undertake an obligation and warranty to install the certificates only on servers that are accessible at the subjectAltName(s) listed in the certificates.
- Subscribers of EV code signing certificates shall promptly request the revocation of their certificates by GDCA in case of the following situations: 1) any information in the certificate is or becomes incorrect or inaccurate; 2) there is any misuse or compromise of the subscriber's private key associated with the public key included in the certificate; 3) there is evidence that such code signing certificates are used to sign suspicious codes.

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

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

- Abide by all provisions of this CPS.
- Ensure that the certificate is used in prescribed scope and duration.
- Verify certificate's trust chain before trust the certificate.
- Before trust a certificate, verify whether the certificate is revoked or not through querying CRL or OCSP.
- The relying party is willing to compensate GDCA for the losses and accept liabilities for any loss of self or others, due to negligence or other reasons violating the terms of a reasonable inspection.
- Prohibited for rejecting any statements, changes, updates and upgrades published by GDCA, including but not limited to modification of strategies and standards as well as additions and deletions of certificate services.

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

GDCA 从事电子认证活动的其他参与者作出如下承诺：

遵守本 CPS 的所有规定。

Other participants engaged in GDCA electronic certification activities make the following commitments:

Abide by all provisions of this CPS.

9.7. 担保免责 Disclaimers of Warranties

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

- 不保证证书订户、信赖方、其他参与者的陈述内容。
- 不对电子认证活动中使用的任何软件做出保证。
- 不对证书在超出规定目的以外的应用承担任何责任。
- 对由于不可抗力，如战争、自然灾害等造成的服务中断并由此造成的客户损失承担责任。
- 订户违反本 CPS9.6.3 之承诺时，或依赖方违反本 CPS9.6.4 之承诺时，得以免除 GDCA 之责任。

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

- Do not guarantee the statements of certificate subscribers, relying party and other.

- Do not guarantee any software used in electronic certification activities.
- Do not assume any liability when certificate is used beyond the prescribed purposes.
- Do not assume any responsibility for service interruption and customer losses caused by force majeure, such as war, natural disasters, etc.
- When subscriber violates the commitments defined in CPS Section 9.6.3, or relying party violates the commitments defined inks Section 9.6.4, GDCA can exempt from liability.

9.8. 有限责任 Limitations of Liability

证书订户、依赖方因 GDCA 提供的电子认证服务从事民事活动遭受损失，GDCA 将承担不超过本 CPS9.9 规定的有限赔偿责任。

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

9.9. 赔偿 Indemnities

9.9.1. GDCA 的赔偿责任 Indemnification by GDCA

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

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

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

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

另外，GDCA 赔偿限制如下：

1. GDCA 所有的赔偿义务不得高于 GDCA 所承担的上限额度，这种赔偿上限可以由 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. 对于由订户或依赖方的原因造成的损失，GDCA 不承担责任，由订户或依赖方自行承担。
3. GDCA 只有在证书有效期限内承担损失赔偿责任。

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

1. All the compensation obligation of GDCA shall not exceed the upper limit what GDCA can afford. The maximum amount of compensation can be reset by GDCA based on different situations. GDCA will notify related parties immediately after the reset.
2. For the losses caused by subscribers or relying party, GDCA does not assume responsibilities. Subscribers or relying themselves should assume their own responsibilities.
3. GDCA assumes the liability for damages only when the certificate is valid.

9.9.2. 订户的赔偿责任 Indemnification by Subscribers

如因下述情形而导致 GDCA 或依赖方遭受损失，订户应当承担赔偿责任：

1. 订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致 GDCA 及其授权的证书服务机构或者第三方遭受损害；
2. 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知 GDCA 及其授权的证书服务机构，以及不当交付他人使用造成 GDCA 及其授权的证书服务机构、第三方遭受损害；

3. 订户使用证书的行为，有违反本 CPS 及相关操作规范，或者将证书用于非本 CPS 规定的业务范围；
4. 证书订户或者其它有权提出吊销证书的实体提出吊销请求后，到 GDCA 将该证书吊销信息予以发布的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果 GDCA 按照本 CPS 的规范进行了有关操作，那么该证书订户必须承担所有损害赔偿责任；
5. 证书中的信息发生变更但未停止使用证书并及时通知 GDCA 和依赖方；
6. 没有对私钥采取有效的保护措施，导致私钥丢失或被损害、窃取、泄露等；
7. 在得知私钥丢失或存在危险时，未停止使用证书并及时通知 GDCA 和依赖方；
8. 证书到期但仍在使用证书；
9. 订户的证书信息侵犯了第三方的知识产权；
10. 在规定的范围外使用证书，如从事违法犯罪活动；

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

1. GDCA and its authorized service agencies or third-party suffer losses due to unreal information, such as deliberate, negligent or malicious provision of unreal information by applicants when applying for certificates.
2. GDCA and its authorized service agencies or third-party suffer losses due to disclosure and loss of private keys deliberately and by mistake; due to not informing GDCA and its authorized service agencies or third-party of the leakage and loss of private keys with knowing the facts; and due to handing keys to others inappropriately.
3. Subscribers violate the CPS and related operation practices when using certificates as well as using the certificates activities outside of the CPS.
4. If the certificate is used for illegal transactions or causes disputes during the period from revocation requests submitted by the subscribers or other entities authorized by GDCA to this information of certificate revocation published by GDCA, if GDCA operates in accordance with the requirements of the CPS, subscribers must assume any responsibility of losses according to this CPS.
5. Subscribers continue to use the certificates and do not notify GDCA and relying parties promptly when information in the certificates is changed.
6. The private key is lost, compromised, stolen, disclosed, and etc. due to not taking effective protection measures.
7. Subscribers continue to use the certificates and do not notify GDCA and relying parties promptly when they are made aware that private keys are lost or at the risk of being compromised.
8. The certificate has expired but is still in use.

9. The subscriber's certificate information infringes upon the intellectual property rights of a third-party.
10. Using certificates beyond specified scope, such as the use of certificates for illegal and criminal activities.

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

如因下述情形而导致 GDCA 或订户遭受损失，依赖方应当承担赔偿责任：

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

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

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

9.10. 有效期限与终止 Term and Termination

9.10.1. 有效期限 Term

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

This CPS will enter into force at 12 o'clock midnight of the effective date, and the last version CPS will become invalid. This CPS will become invalid when the next version CPS enters into force or

the electronic certification services of GDCA are terminated.

9.10.2. 终止 Termination

在 GDCA 终止电子认证服务时，本 CPS 终止。

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

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

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

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

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

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

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

9.12. 修订 Amendments

9.12.1. 修订程序 Procedure for Amendment

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

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

As authorized by GDCA Security Policy Committee, CPS composition team reviews this CPS at

least once a year to ensure that the CPS meets the requirements of national laws and regulations and administration department as well as relevant international standards; to ensure it meets the requirements of CP and actual needs of certification business operations.

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

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

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

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

9.12.3. 必须修改业务规则的情形 Circumstances Under Which CPS Must be Changed

GDCA 必须对本 CPS 进行修改的情形包括：CPS 中相关内容与管辖法律的不一致，国家监管部门对本机构认证业务有明确的更改或调整要求等。

The situations that GDCA must modify this CPS include: discrepancies between CPS and governing laws, clear requirements of changes or adjustments for GDCA certification services initiated by national regulatory departments.

9.12.4. 对象标识符变更 Object Identifier Modification

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

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

9.13. 争议处理 Dispute Resolution Provisions

GDCA、证书订户、依赖方等实体在电子认证活动中产生争议可按以下步骤解决：

1. 根据本 CPS 中的规定，明确责任方；

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

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

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

9.14. 管辖法律 Governing Law

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

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

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

无论 GDCA 的证书订户、依赖方等实体在何地居住以及在何处使用 GDCA 的证书，本 CPS 的执行、解释和程序有效性均适用中华人民共和国的法律。任何与 GDCA 或授权注册机构就本 CPS 所涉及的任何争议，均适应中华人民共和国法律。

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

9.16. 一般条款 Miscellaneous Provisions

9.16.1. 完整协议 Entire Agreement

GDCA 的 CPS 完整的文档结构包括：标题、目录、主体内容 3 部分。关于对目录

和主体内容修改后的替代内容，将完全代替所有先前部分、并被放置在 GDCA 的网站中以供查阅和浏览。

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

9.16.2. 转让 Assignment

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

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

9.16.3. 分割性 Severability

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

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

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

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

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

available at https://cabforum.org/pipermail/public/.

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

9.16.4. 强制执行 Enforcement

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

GDCA declares that if the subscribers or relying parties did not execute any item within this CPS, it should not be consider that they need not to be executed in the future.

9.16.5. 不可抗力 Force Majeure

GDCA 不对因战争、瘟疫、火灾、地震和其他天灾等不可抗力的事件所造成本 CPS 规定担保责任的违反、延误或无法履行负责。

GDCA do not assume responsibilities for losses incurred by the violation, delay or inability to perform the CPS regulations due to the force majeure events like wars, epidemics, fires, earthquakes and other natural disasters.

9.17. 其他条款 Other Provisions

GDCA 对本 CPS 具有最终解释权。

GDCA has final interpretation rights to this CPS.

附录 1：证书信息

Appendix 1: Certificate information

Root/CA Certificate	Information
GDCA TrustAUTH R5 ROOT	Country =CN Organization = GUANG DONG CERTIFICATE AUTHORITY CO., LTD. Common Name = GDCA TrustAUTH R5 ROOT Serial Number= 7d 09 97 fe f0 47 ea 7a Validity：November, 26 2014 to December, 31, 2040 SHA1 digest= 0f 36 38 5b 81 1a 25 c3 9b 31 4e 83 ca e9 34 66 70 cc 74 b4
GDCA TrustAUTH R4 EV SSL CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name = GDCA TrustAUTH R4 EV SSL CA Serial Number = 02 92 33 24 6b c6 31 4b Validity：April, 6 2016 to December, 31, 2030 SHA1 digest= c6 7a 61 4f 23 42 18 b7 9f be 91 40 c0 33 dc aa 73 2a 5c 4f
GDCA TrustAUTH R4 EV CodeSigning CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name = GDCA TrustAUTH R4 EV CodeSigning CA Serial Number = 63 54 b0 a6 f5 ff 59 2a Validity：April, 7 2016 to December, 31, 2030 SHA1 digest= d5 6c 4f fb 6d c9 d1 c2 6d 98 a0 57 2a 75 24 80 71 cf 72 9d
数安时代 R5 根 CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name =数安时代 R5 根 CA Serial Number = 2e d9 58 82 91 39 ad 07 Validity：March, 31 2016 to December, 31, 2040 SHA1 digest= 23 eb 1b a4 64 71 a1 e7 e9 f2 db 57 01 fe f8 f2 f8 0c aa e9
数安时代 R4 EV 服务器证书 CA	Country =CN Organization= Global Digital Cybersecurity Authority Co., Ltd.

	Common Name =数安时代 R4 EV 服务器证书 CA Serial Number = 64 35 81 b4 22 f5 d1 06 Validity：March, 31 2016 to December, 31, 2030 SHA1 digest= 0d 9d 15 af 72 5b eb a2 27 c4 29 43 23 10 c5 53 b7 b8 9b d3
GDCA TrustAUTH E5 ROOT	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name = GDCA TrustAUTH E5 ROOT Serial Number = 1a f5 1f 4d 2c da bb 53 Validity：March, 23 2016 to December, 31, 2040 SHA1 digest= eb 46 6c d3 75 65 f9 3c de 10 62 cd 8d 98 26 ed 23 73 0f 12
GDCA TrustAUTH E4 EV SSL CA	Country =CN Organization = Global Digital Cybersecurity Authority Co., Ltd. Common Name = GDCA TrustAUTH E4 EV SSL CA Serial Number = 0c 50 cc c1 d3 f7 14 7f Validity：March, 31 2016 to December, 31, 2030 SHA1 digest= 1f ae a7 c3 5e 84 b9 5a 55 f6 c7 d7 fd 2f e5 21 ea 77 72 59

附录 2：GDCA EV 证书电子认证业务规则修订记录表

Appendix 2: GDCA EV CPS Revision Records

内容 / 序号	修订章节	V1.6	V1.7	备注说明
1	1.2. 文档名称与标识		披露版本信息描述。	
2	3.2.2.机构身份的鉴别 Authentication of Organization Identity		域名确认部分：删除 Baseline Requirments v1.4.1 第 3.2.2.4.5 节的验证方式；调整 Baseline Requirments 版本号；披露 Baseline Requirments v1.5.6 第 3.2.2.4.7 节的验证方式。	
3	5.5.5.记录时间戳要求 Requirements for Time-Stamping of Records	GDCA 的档案在创建的时候须加盖带有 GDCA 数字签名的时间戳。	调整描述为“GDCA 的归档记录都需要标注时间，系统产生的记录按要求添加时间标识。”	
4	其他修订		修订一些语言描述及文字上错误及其他一些容易引起歧义的地方。 根据 RFC3647 结构对 CPS 进行了一些调整。	

Contents / SEQ	Sections Revised	V1.6	V1.7	Remarks
1	1.2. 文档名称与标识 Document Name and Identification		Added description on CPS version.	
2	3.2.2.机构身份的鉴别 Authentication of Organization Identity		Deleted validation method 3.2.2.4.5 of the Baseline Requirments v1.4.1. Adjusted the version number of the Baseline Requirments, and added validation method 3.2.2.4.7 of the Baseline Requirments v1.5.6.	

3	5.5.5.记录时间戳要求 Requirements for Time-Stamping of Records	“The GDCA file must be created with time-stamped signed by GDCA digital signatures.”	Changed to “The archived records of GDCA are labeled with time, and the records generated by the system are required to be added a time stamp.”	
4	Other revisions		Corrected a few mistakes, adjusted some wording issues, and other parts that may cause confusion. Minor adjustions as per the RFC 3647 structure.	