东方新诚信数字认证中心

电子认证服务业务规则

Version 2.0



东方新诚信数字认证中心有限公司

二〇二六年十月

目 录

1 概括性描述 1
1.1 承诺 1
1.2 基本信息 1
1.3 文档名称与标识 3
1.3.1 文档基本信息 3
1.3.2 历史版本信息 3
1.4 电子认证活动参与者 5
1.4.1 电子认证服务机构 5
1.4.2 注册机构 5
1.4.3 业务受理点 6
1.4.4 订户 6
1.4.5 依赖方 6
1.4.6 其他参与者 7
1.5 证书应用 7
1.5.1 数字证书类型概述 7
1.5.2 电子签名认证证书 7
1.6 策略管理 9
1.6.1 策略管理机构 9
1.6.2 CPS 批准程序 10
1.7 定义和缩写 11
2 信息发布与信息管理 14
2.1 认证信息的内容 14
2.2 信息发布方式 14
2.3 监管备案 15
2.4 证书信息对接 15
2.5 发布的时间与频率 15
2.6 信息库访问控制 15
3 身份标识与查验 17
3.1 身份查验通用要求 17
3.1.1 通用要求 17
3.1.2 订户告知 17
3.2 初始身份确认 18
3.2.1 证明拥有私钥的方法 18
3.2.2 个人身份的查验 18
3.2.3 机构身份的查验 20
3.3 密钥更新请求的身份标识与鉴别 22
3.3.1 常规密钥更新的标识与鉴别 22
3.3.2 撤销后密钥更新的标识与鉴别 22
3.3.3 证书变更的标识与鉴别 22
3.3.4 撤销请求的标识与鉴别 22
3.4 订户意愿记录 23
3.4.1 订户意愿记录内容 23

3.4.2 个人高等级证书的意愿记录 23
3.4.3 个人基础级证书的意愿记录 23
3.4.4 机构高等级证书的意愿记录 24
3.4.5 机构基础级证书的意愿记录 24
3.5 订户协议 24
3.6 未验证的订户信息 24
3.7 互操作要求 24
3.8 命名 25
4 证书生存周期操作要求 27
4.1 通用要求 27
4.2 证书申请 27
4.2.1 证书申请实体 27
4.2.2 证书申请流程与责任 28
4.3 证书申请处理 28
4.3.1 执行身份确认功能 28
4.3.2 证书申请批准和拒绝 28
4.3.3 证书申请处理时限 29
4.4 证书签发 29
4.4.1 证书签发过程中 DFCA 的行为 29
4.4.2 结果通告 30
4.5 证书接受 30
4.5.1 构成接受证书的行为 30
4.5.2 证书的发布 30
4.5.3 在颁发证书时对其他实体的通告 31
4.6 密钥对和证书的使用 31
4.6.1 密钥对的安全保护 31
4.6.2 订户对私钥和证书的使用 31
4.6.3 依赖方对公钥和证书的使用 32
4.7 证书续期 32
4.7.1 证书续期更新的情形 32
4.7.2 证书续期的申请主体 33
4.7.3 证书续期的申请处理 33
4.7.4 证书签发与接受 33
4.8 证书密钥更新 33
4.8.1 证书密钥更新的情形 33
4.8.2 证书密钥更新的申请主体 34
4.8.3 证书密钥更新的申请处理 34
4.8.4 证书签发与接受 34
4.9 证书变更 34
4.9.1 证书变更的情形 34
4.9.2 证书变更的申请主体 34
4.9.3 证书变更的申请处理 35
4.9.4 证书签发与接受 35
4.10 证书撤销或冻结 35

4.10.1 证书撤销或冻结的情形 35
4.10.2 证书撤销或冻结的申请主体 36
4.10.3 证书撤销或冻结的申请处理 36
4.10.4 注销请求宽限期 36
4.10.5 DFCA 处理注销请求的时限 37
4.10.6 依赖方检查证书注销的要求 37
4.10.7 CRL 发布频率 37
4.10.8 CRL 发布的最大滞后时间 37
4.10.9 ARL 发布频率 37
4.11 证书状态信息服务 38
4.11.1 证书状态信息服务方式 38
4.11.2 证书状态信息服务的可用性 38
4.11.3 备用服务 38
4.12 停止使用认证服务 38
4.12.1 停止使用认证服务的情形 38
4.12.2 停止使用认证服务的处理 38
4.13 密钥托管与恢复 39
4.13.1 密钥托管与恢复概述 39
4.13.2 密钥托管与恢复的策略与行为 40
4.13.3 密钥托管与恢复的策略与行为 40
4.13.4 会话密钥的封装与恢复的策略与行为 40
5 认证机构设施、管理和操作控制 41
5.1 物理控制 41
5.1.1 场地位置与建筑 41
5.1.2 门禁与监控 42
5.1.3 电力与空调 42
5.1.4 灾难备份 43
5.1.5 环境保障 43
5.1.6 消防措施 43
5.1.7 设备管理 44
5.1.8 存储介质管理 44
5.1.9 废物处理 44
5.2 操作过程控制 45
5.2.1 可信角色 45
5.2.2 职责分离 45
5.2.3 每个角色的识别与鉴别 46
5.2.4 需要职责分割的角色 46
5.3 人员控制 46
5.3.1 可信人员资格要求 46
5.3.2 可信人员培训要求 47
5.3.3 工作轮换周期和顺序 48
5.3.4 未授权行为的处罚 48
5.3.5 独立合约人的要求 48
5.3.6 提供给员工的文档 48

5.4 审计日志程序 49
5.4.1 记录事件的类型 49
5.4.2 记录内容 49
5.4.3 保存期限 50
5.4.4 日志审计 50
5.4.5 对导致事件实体的通告 51
5.4.6 脆弱性评估 51
5.5 记录归档 51
5.5.1 归档记录的类型 51
5.5.2 归档记录的保存期限 52
5.5.3 归档文件的保护 52
5.5.4 归档文件的备份程序 52
5.5.5 记录时间戳要求 53
5.5.6 归档收集系统 53
5.5.7 获得和检验归档信息的程序 53
5.6 电子认证服务机构根证书密钥更替 53
5.6.1 密钥更替的情形 53
5.6.2 密钥更替的流程 53
5.7 损害和灾难恢复 54
5.7.1 业务连续性目标 54
5.7.2 事故和损害处理程序 54
5.7.3 恢复流程 54
5.7.4 根私钥应急处理 55
5.7.5 事件报告 56
5.7.6 定期验证 56
5.8 电子认证服务机构终止 56
5.9 重大事项报告 57
5.9.1 重大事项报告的情形 57
5.9.2 重大事项报告的流程与时限 58
6 认证系统技术安全控制 60
6.1 技术安全管理制度要求 60
6.2 密钥对的生成和安装 60
6.2.1 根证书密钥对的生成和安装 60
6.2.2 订户密钥对的生成和交付 60
6.2.3 公钥传送给证书签发机构 61
6.2.4 电子认证服务机构公钥传送给依赖方 61
6.2.5 密钥的长度 61
6.2.6 公钥参数的生成和质量检查 61
6.2.7 密钥使用目的 61
6.3 私钥保护和密码模块工程控制 62
6.3.1 CA 私钥保护和密码模块工程控制 62
6.3.2 订户私钥保护和密码模块工程控制 63
6.4 密钥对管理的其他方面 64
6.4.1 公钥归档 64

6.4.2 证书操作期和密钥对使用期限 64
6.5 激活数据 64
6.6 计算机安全控制 65
6.6.1 特别的计算机安全技术要求 65
6.6.2 计算机安全评估 65
6.7 生存周期安全控制 66
6.7.1 系统开发控制 66
6.7.2 安全管理控制 66
6.7.3 生命期的安全控制 66
6.8 网络安全控制 66
6.9 时间戳 67
7 证书、证书撤销列表和在线证书状态协议 68
7.1 证书 68
7.2 证书撤销列表 68
7.3 在线证书状态协议 69
8 认证机构审计及相关评估 70
8.1 审计评估制度 70
8.1.1 审计评估的类型与方式 70
8.1.2 审计评估的频率 71
8.1.3 外部审计机构的要求 71
8.1.4 外部审计机构的审计人员的专业要求 71
8.2 认证业务审计 72
8.3 全面符合性评估 72
9 法律责任和其他业务条款 74
9.1 费用 74
9.2 财务责任 74
9.2.1 保险范围 74
9.2.2 资金保障与管理 75
9.3 业务信息保密 75
9.3.1 不属于保密的信息 75
9.3.2 保护保密信息的责任 76
9.4 个人隐私保护 76
9.4.1 隐私保密方案 76
9.4.2 作为隐私处理的信息 76
9.4.3 不被视为隐私的信息 77
9.4.4 保护隐私的责任 77
9.4.5 使用隐私信息的告知与同意 77
9.4.6 依法律或行政程序的信息披露 77
9.4.7 其他信息披露情形 77
9.5 知识产权 77
9.6 陈述和担保 78
9.6.1 电子认证服务机构的陈述与担保 78
9.6.2 RA 的陈述与担保 78
9.6.3 订户的陈述与担保 79

9.6.4 依赖方的陈述与担保 79
9.6.5 其他参与者的陈述与担保 79
9.7 担保免责 80
9.8 偿付责任规则 81
9.9 赔偿 81
9.9.1 赔偿范围 81
9.9.2 赔偿限额 82
9.9.3 赔偿处理时限 83
9.10 有效期和终止 83
9.10.1 有效期限 83
9.10.2 终止 84
9.10.3 效力的终止与保留 84
9.11 对参与者的个别通告与沟通 84
9.12 修订和发布 84
9.12.1 修订程序 84
9.12.2 通知机制和期限 84
9.12.3 必须修改业务规则的情形 85
9.13 争议处理与举证 85
9.13.1 总体说明 85
9.13.2 争议解决机制 85
9.13.3 全生命周期举证制度与能力体系 87
9.13.4 举证服务时间承诺 88
9.13.5 举证责任与免责说明 88
9.14 管辖法律 89
9.15 与适用法律的符合性 89
9.16 一般条款 89
9.16.1 完整协议 89
9.16.2 转让 89
9.16.3 分割性 89
9.16.4 强制执行 89
9.16.5 不可抗力 90
9.17 其他条款 90

DongFang eTrusted Certification Authority Center of China
东方新诚信数字认证中心
.DFCA.

1 概括性描述

1.1 承诺

东方新诚信数字认证中心有限公司（以下简称为“东方新诚信 CA”、“DFCA”）是经国家主管部门行政许可审批而设立的、专业从事电子认证服务的第三方服务机构，面向各行各业的数字化转型、人工智能、可信数据空间，以及电子政务、电子商务等在线服务应用领域，提供证书管理、密钥管理等基础电子认证服务，提供涵盖“身份认证、授权管理、责任认证、数据安全”等扩展的电子认证应用支撑服务。

作为专业的电子认证服务机构，DFCA 面向所有客户郑重承诺：

1. 开展经营活动和服务活动时，遵循《中华人民共和国电子签名法》与《电子认证服务管理办法》等法律与行政法规的要求，树立以人民为中心的服务理念，承担社会责任；
2. 与客户建立业务关系前，秉承“应用为王、安全并重”的宗旨，开展电子认证服务在应用的业务调研，建立应用接入业务风险评估及内部定责机制，严禁为存在违法违规风险的业务提供电子认证服务；
3. 遵循国家《商用密码管理条例》的要求，使用经过国家密码管理局审查的电子认证服务系统、密码设备等安全系统，为客户提供安全、可信的电子认证服务；
4. 主动接受政府与社会各界监督，持续完善电子认证服务的业务模式。建立问题长效纠治与持续更新机制，对主管部门检查发现的问题与客户反馈的意见，依规及时落实与整改，确保服务合规开展、系统稳定运行。

1.2 基本信息

1. 机构名称：东方新诚信数字认证中心有限公司
2. 统一信用代码：914301007225709294
3. 法定代表人：杜国伟
4. 机构住所与经营场所：湖南省长沙市高新技术开发区麓龙路 199 号（邮编：410205）
5. 联系方式：0731-85501716，0731-85501816

6. 《电子认证服务许可证》：

(1) 许可证编号：ECP43010422034

(2) 发证机关：中华人民共和国工业和信息化部

(3) 批准日期：2022 年 10 月 18 日

(4) 有效期：2022 年 10 月 19 日至 2027 年 10 月 18 日

7. 证书链

(1) 社会公众应用根证书(SM2)：

- 证书序列号：2bb5b8c349b031919fc0c67967dfe7c2
- 颁发机构名称：国家密码管理局
- 颁发者：CN = ROOTCA, O = NRCAC, C = CN
- 密码算法：SM3WithSM2
- 密钥长度：256bit
- 使用者：CN = ROOTCA, O = NRCAC, C = CN
- 有效期：2012年7月14日 11:11:59~2054年7月7日 11:11:59
- 计划服务时间：长期

(2) 东方新诚信 CA 运营 CA 证书：

- 证书序列号：59754daa8f9d8105432354f866378655
- 颁发机构名称：国家密码管理局
- 颁发者：CN = ROOTCA, O = NRCAC, C = CN
- 密码算法：SM3WithSM2
- 密钥长度：256bit
- 使用者：CN = DongFang eTrust CA, O = DongFang Electronic Certificate Center, L = Changsha, S = Hunan, C = CN
- 有效期：2013年6月4日 12:42:07~2033年5月30日 12:42:07
- 计划服务时间：长期

1.3 文档名称与标识

1.3.1 文档基本信息

1. 文档名称：《东方新诚信数字认证中心电子认证服务业务规则》，以下简称“本CPS”
2. 文档版本：Version 2.0
3. CPS OID：1.2.156.115221
4. 发布日期：2026 年 6 月 20 日
5. 遵循的证书策略 OID：DFCA 采用国家统一规定的证书策略 OID：
   (1) 个人高等级电子签名认证证书：2.16.156.339.2.1.1.2
   (2) 个人基础级电子签名认证证书：2.16.156.339.2.1.1.1
   (3) 机构高等级电子签名认证证书：2.16.156.339.2.1.2.2
   (4) 机构基础级电子签名认证证书：2.16.156.339.2.1.2.1

1.3.2 历史版本信息

1.3.2.1 Version 2.0 对 Version 1.8 的修订

遵循《电子认证业务规划规范》的要求，从文档结构、文档内容等方面，对原 Version 1.8 进行了全面修改。主要增加与修改内容如下：

1. “1.4.2 注册机构”，只能由 DFCA 设立，不可授权或委托其他机构设立注册机构；
2. “1.5 证书应用”，增加“1.5.2 电子签名认证证书”的类型、适用范围、应用限制
3. “1.5 证书应用”，删除“常规数字证书、社保卡应用证书、社保卡副本证书、嵌入式设备证书、服务器证书”等证书的内容；
4. 根据《电子认证业务规划规范》要求，修改了 1.6、1.7 的相关内容；
5. 根据《电子认证业务规划规范》要求，修改了“2. 信息发布与信息管理”相关内容；
6. 根据《电子认证业务规划规范》要求，修改了“3. 身份标识与查询”的目录结构；

7. 增加了“3.1 身份查验通用要求”；
8. 根据《电子认证业务规划规范》要求，修改了“3.2 初始身份确认”的内容，增加了四类“电子签名认证证书”的初始身份确认的要求，删除了“常规数字证书、社保卡应用证书、社保卡副本证书、嵌入式设备证书、服务器证书”等证书的内容；
9. 根据《电子认证业务规划规范》要求，增加了“3.3.2 撤销后密钥更新的标识与鉴别”、“3.3.3 证书变更的标识与鉴别”；
10. 增加“3.4 订户意愿记录”、“3.5 订户协议”、“3.7 互操作要求”；
11. 根据《电子认证业务规划规范》要求，修改了“4. 证书生存周期操作要求”的目录结构与相关内容；
12. 删除了“4. 证书生存周期操作要求”中“常规数字证书、社保卡应用证书、社保卡副本证书、嵌入式设备证书、服务器证书”等证书的内容；
13. 根据《电子认证业务规划规范》要求，修改了“5. 认证机构设施、管理和操作控制”的目录结构与相关内容；
14. 根据《电子认证业务规划规范》要求，修改了“6. 认证系统技术安全控制”的目录结构与相关内容；
15. 根据《电子认证业务规划规范》要求，修改了“7. 证书、证书撤销列表和在线证书状态协议”的目录结构与相关内容；
16. 根据《电子认证业务规划规范》要求，修改了“8. 认证机构审计及相关评估”的目录结构与相关内容；
17. 根据《电子认证业务规划规范》要求，修改了“9. 法律责任和其他业务条款”的目录结构与相关内容。

1.3.2.2 Version 1.8 对 Version 1.7 的修订

1. 增加“1.3 本次修订主要内容”，补充 Version1.8 对 Version 1.7 的修订内容说明。后续修订将增加对修订内容的说明；

注：该章节为 Version 1.8 后新增，Version1.7 以前的修订内容不予以体现。

2. “1.5.1 适合的证书应用”，增加“1.5.1.6 服务器证书”；
3. “3.2.1 证明拥有私钥的方法”，增加“3.2.1.5 服务器证书”；
4. “3.2.2 组织机构身份的鉴别”，增加“3.2.2.5 服务器证书”；

5. “3.2.3 个人身份的鉴别”，增加“3.2.3.5 服务器证书”；
6. “3.2.4 域名的确认”，增加“3.2.4.5 服务器证书”；
7. “3.2.6 授权确认”，增加“3.2.6.5 服务器证书”；
8. “3.4.1 订户个人撤销请求”，增加“3.4.1.5 服务器证书”；
9. “4.1.1 证书申请实体”，增加“4.1.1.5 服务器证书”；
10. “4.1.2 证书申请过程”，增加“4.1.2.5 服务器证书”；
11. “4.1.3 责任”，增加“4.1.3.5 服务器证书”；
12. “4.2.1 执行识别与鉴别功能”，增加“4.2.1.5 服务器证书”；
13. “4.2.3 处理证书申请时间”，增加“4.2.3.5 服务器证书”；
14. “4.3.1 证书签发过程中的 DFCA 行为”，增加“4.3.1.5 服务器证书”；
15. “4.3.2 DFCA 对订户的通告”，增加“4.3.2.5 服务器证书”；
16. “4.4.1 构成接受证书的行为”，增加“4.4.1.5 服务器证书”；
17. “4.9.1 证书撤销的情形”，增加“4.9.1.5 服务器证书”；
18. “4.9.3.1 订户撤销申请”，增加“4.9.3.1.5 服务器证书”；
19. “4.12.1.1 密钥托管策略与行为”，增加“4.12.1.1.5 服务器证书”。

1.4 电子认证活动参与者

1.4.1 电子认证服务机构

DFCA 是根据《中华人民共和国电子签名法》和《电子认证服务管理办法》规定，依法建设的第三方电子认证服务机构。

电子认证服务机构是受订户信任，负责对证书的签发、发布、更新、撤销等证书全生命周期进行管理的实体。

1.4.2 注册机构

注册机构（以下简称为“RA”）是由电子认证服务机构设立的、负责受理证书申请、审核、更新、撤销等各类证书业务的处理的业务机构。

RA 必须根据本 CPS 开展相关证书业务服务。DFCA 根据业务发展需要，对业务的地

域、行业、证书发展规模等进行严格的评估审计后，由安全策略委员会最终决定而设立。

RA 有责任妥善保存与保管订户的数据，不允许将订户数据透露给与证书申请无关的任何单位或个人，不允许将订户数据用于商业利益方面的用途。RA 对其提供的证书服务负有相关的法律责任，包括但不限于本 CPS 和授权协议中所规定的有关内容。

1.4.3 业务受理点

业务受理点（LRA）是经过 DFCA 或其注册机构的审查后设立，负责办理证书的申请、更新、撤销、下载及其他授权业务。LRA 对其提供的证书服务的受理过程负有相关的法律责任，包括但不限于本 CPS 和授权协议中所规定的有关内容。

1.4.4 订户

订户，即证书持有人，是指从 DFCA 接收证书的实体。包括已经申请并拥有 DFCA 签发的数字证书的单位、企业、组织、机构、个人、服务器、网站等各类主体或实体，以及其他任何具有确定的身份标识，并持有 DFCA 签发的数字证书的对象。

在电子签名应用中，订户即为电子签名人。

1.4.5 依赖方

依赖方是指任何使用 DFCA 签发的证书进行网络作业的证书持有者和按照本 CPS 合理信任证书真实性的实体。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。

在 DFCA 的证书服务体系中，依赖方是信任 DFCA 所签发的数字证书（以下简称为“东方新诚信证书”），可以对使用东方新诚信数字证书机制生成的数字签名进行验证，使用其他东方新诚信证书的公钥的实体。依赖方可以在法律规定以及本 CPS 规定的范围内信任证书及其签名，并享有本 CPS 规定的各种权利。

依赖方应合理地信任证书以及相关的数字签名。如果信任数字签名时需要额外的保证，依赖方必须得到这些保证后才能合理地信任该数字签名。

非 DFCA 订户的依赖方，DFCA 除了担保其所信任的并且由 DFCA 签发的证书和相关

签名信息的真实性以外，不承担其它义务和责任。

1.4.6 其他参与者

其他参与者是指其他为 DFCA 提供相关服务或使用 DFCA 所提供的服务的实体。

1.5 证书应用

1.5.1 数字证书类型概述

东方新诚信 CA 所签发的数字证书能够满足各行各业的数字化转型、人工智能、可信数据空间、电子政务、电子商务等在线服务应用领域等应用领域对电子认证服务的需要。证书申请人根据实际需要，决定采用哪种类型的数字证书。

东方新诚信 CA 所签发的数字证书主要包括以下类型：

1. 电子签名认证证书

电子签名认证证书是指遵循《中华人民共和国电子签名法》、《电子认证服务管理办法》等法律法规与管理办法，以及《电子认证业务规则规范》等标准规范，所签发的数字证书（亦简称为“电子签名证书”）。

1.5.2 电子签名认证证书

1.5.2.1电子签名认证证书类型

电子签名认证证书符合《中华人民共和国电子签名法》的要求。

按证书主体对象的类型和风险等级，电子签名认证证书具体分为个人高等级电子签名认证证书、个人基础级电子签名认证证书、机构高等级电子签名认证证书、机构基础级电子签名认证证书四种类型。

1. 个人高等级电子签名认证证书：面向个人用户，在证书申请时，采用高强度的身份鉴别机制对业务申请、申请者（或经办人）身份进行鉴证而签发的电子签名认证证书，证书策略 OID 为 2.16.156.339.2.1.1.2（主管部门证书策略 OID）。该类证书适用于高风险业务，例如，金融、保险等高风险的业务办理、重要数据或敏感信息的提交、变更等；

2. 个人基础级电子签名认证证书：面向个人用户，在证书申请时，采用基本的身份鉴别机制对业务申请、申请者（或经办人）身份进行鉴证而签发的电子签名认证证书，证书策略 OID 为 2.16.156.339.2.1.1.1（主管部门证书策略 OID）。该类证书适用于低风险业务，例如，用户注册、非重要或非敏感信息（如：统计数据、个人邮箱等）的提交、变更等；

3. 机构高等级电子签名认证证书：面向机构用户或机构所属的工作人员，在证书申请时，采用高强度的身份鉴别机制对业务申请、申请者（或经办人）身份进行鉴证而签发的电子签名认证证书，证书策略 OID 为 2.16.156.339.2.1.2.2（主管部门证书策略 OID）。该类证书适用于高风险业务，例如，金融、保险等高风险的业务办理、重要数据或敏感信息的提交、变更等；

4. 机构基础级电子签名认证证书：面向机构用户或机构工作人员，在证书申请时，采用基本的身份鉴别机制对业务申请、申请者（或经办人）身份进行鉴证而签发的电子签名认证证书，证书策略 OID 为 2.16.156.339.2.1.2.1（主管部门证书策略 OID）。该类证书适用于低风险业务，例如，用户注册、非重要或非敏感信息（如：统计数据、个人邮箱等）的提交、变更等；

电子签名认证证书分类，具体见表 1-1。

表 1-1 电子签名认证证书类型

证书类型	证书策略 OID	含义
个人高等级电子签名认证证书	2.16.156.339.2.1.1.2	适用于高风险业务，符合《电子签名法》的个人电子签名认证证书
个人基础级电子签名认证证书	2.16.156.339.2.1.1.1	适用于低风险业务，符合《电子签名法》的个人电子签名认证证书
机构高等级电子签名认证证书	2.16.156.339.2.1.2.2	适用于高风险业务，符合《电子签名法》的机构电子签名认证证书
机构基础级电子签名认证证书	2.16.156.339.2.1.2.1	适用于低风险业务，符合《电子签名法》的机构电子签名认证证书

1.5.2.2 电子签名认证证书适用的应用场景

1. 电子签名

采用东方新诚信证书对信息进行电子签名，实现对信息的完整性保护，防止对信息的篡改。同时，还可实现提交信息的不可抵赖性。通过在电子签名时包含时间信息，还可形成时间戳签名，实现对关键操作的时间进行真实性验证。

2. 身份认证

保证采用 DFCA 信任服务的证书持有者身份的合法性，主要包括对个人、机构和设备等网络实体的鉴别。

3. 信息保护

对于信息化应用中存储与传输的重要信息、敏感信息，可以采用东方新诚信证书进行加密保护。

4. 权限管理

以东方新诚信证书作为订户身份认证的凭证，在此基础上，对订户进行分组划分，进而对其进行权限管理与访问控制。

1.5.2.3 电子签名认证证书应用限制

电子签名认证证书的使用应符合证书内容对其用途的限定，如参与方未经 DFCA 认可或不遵守相关约定，其对证书的应用超出限定的应用范围，将不受 DFCA 的保护。电子签名认证证书禁止使用的场景，包括但不限于：

1. 涉及人身关系的，如婚姻、收养、继承等；
2. 涉及停止公共事业服务的，如停止供水、供热、供气等；
3. 法律、行政法规规定的其他不适用电子签名的应用场景或类型；
4. 国家法律法规禁止的活动；
5. 涉及生命健康、财产权产权益等高风险活动禁止使用基础级电子签名认证证书。

1.6 策略管理

1.6.1 策略管理机构

1.6.1.1 策略管理机构职责

本 CPS 的管理机构是 DFCA 安全策略委员会。安全策略委员会负责 CPS 和 CP 以及配套制度的管理，包括但不限于以下职责：

1. 确定维护 CPS 和 CP 等策略文档的职能分工，建立合理有效的修订和批准流程；
2. 对涉及信息安全策略、根证书密钥、证书签发自动审核等重要操作和流程进行审批；

3. 每年至少进行一次 CPS 和 CP 全面评审，根据实际需要及时修订策略文档；
4. 每年组织运营风险评估并形成报告。

1.6.1.2 策略管理机构人员名单

DFCA 在官方门户网站（https://www.dfca.cn）对安全策略委员会成员予以公示。

1.6.2 CPS 批准程序

1.6.2.1 CPS 批准程序概述

DFCA 安全策略委员会负责 CPS 的批准管理。具体流程包括：起草小组的成立流程、安全策略委员会的审批流程、主管机关的 CPS 备案流程、CPS 发布流程。

1.6.2.2 起草小组的成立流程

安全策略管理委员会负责指定 CPS 起草小组，经安全策略委员会会议审议后正式成立 CPS 起草小组。

1.6.2.3 安全策略委员会的审批流程

安全策略委员会负责 CPS 审批，具体流程如下：

1. 起草小组完成 CPS 起草或修订，形成讨论稿；
2. 起草小组就讨论稿向公司内各部门征求意见；
3. 起草小组就各部门反馈的意见，与相关方进行交流与讨论，达成一致意见后，对讨论稿进行修改，形成送审稿；
4. 起草小组向安全策略委员会提交送审稿，申请评审；
5. 安全策略委员会组织评审会，对送审稿进行评审，形成评审意见。必要时，可邀请外部专家参加；
6. 起草小组根据评审意见进行修改，形成报批稿并提交安全策略委员会审批；
7. 安全策略委员会召开安全策略委员会会议，经会议审批通过后，签署审批意见，并

确定正式生效日期。

1.6.2.4 主管机关的 CPS 备案流程

根据电子认证服务管理办法的要求，CPS 发生变动时，DFCA 需将 CPS 向国家工业和信息化部备案。CPS 备案流程如下：

1. 根据安全策略委员会的审批意见，DFCA 综合管理部门按公司关于公文的行政管理要求，完成“CPS 备案公文”的起草、审稿、定稿。“CPS 备案公文”将审批通过的 CPS 作为附件；
2. DFCA 综合管理部门将按正式定稿的“CPS 备案公文”，按要求上报至国家电子认证服务的主管机关；
3. 主管机构的 CPS 备案工作在 CPS 发布之日起 30 天内完成。

1.6.2.5 CPS 发布流程

CPS 经安全策略委员会审批通过后，由系统运维部门将生成 CPS 的电子文档，在公司官网对外发布。

1.7 定义和缩写

1.7.1.1 术语定义

下列定义适用于本 CPS：

1. 东方新诚信数字认证中心

受订户信任，负责创建和分配订户密钥和公钥证书的权威机构。

2. 东方新诚信数字认证中心电子认证服务业务规则

关于东方新诚信数字证书电子认证服务机构在签发、管理、撤销或更新证书（或更新证书中的密钥）过程中采纳的业务实践的声明。

3. 注册机构

具有下列一项或多项功能的实体：识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动撤销或冻结证书，处理订户撤销或冻结证书的请求，同意或拒绝订户更新其证

书或密钥的请求。

4. 数字证书

亦简称为证书，包含公开密钥拥有者的信息，公开密钥，签发者信息、有效期，以及一些扩展信息的数字文件。

5. 电子签名认证证书

亦简称为电子签名证书，遵循《中华人民共和国电子签名法》、《电子认证服务管理办法》等法律法规与管理办法，以及《电子认证业务规则规范》等标准规范，所签发的数字证书。

6. 证书撤销列表（CRL）

一个已标识的列表，它指定了一套证书发布者认为无效的证书。除普通 CRL 外，还定义了一些特殊的 CRL 类型用于覆盖特殊领域的 CRL。

7. CA 机构撤销列表（ARL）

一个经电子认证服务机构数字签名的列表，标记已经被撤销的 CA 的公钥证书的列表，表示这些证书已经无效。

8. 私钥

私钥是指在公钥密码系统中，订户的密钥对中只能由订户持有并保持为秘密的密钥。

9. 公钥

公钥是指在公钥密码系统中，订户的密钥对中可以公开的密钥。

1.7.1.2 缩略语

CA 电子认证服务机构（Certification Authority）

CP 证书策略（Certificate Policy）

CPS 电子认证业务规则（Certificate Practice Statement）

CRL 证书撤销列表（Certificate Revocation List）

DN 甄别名（Distinguished Name）

LDAP 轻量级目录访问协议（Lightweight Directory Access Protocol）

LRA 本地注册机构（Local Registration Authority）

OCSP 在线证书状态协议（Online Certificate Status Protocol）

OID 对象标识符（Object Identifier）

RA 注册机构（Registration Authority）

RTO 恢复时间目标（Recovery Time Objective）

RPO 恢复点目标（Recovery Point Objective）

2 信息发布与信息管理

2.1 认证信息的内容

DFCA 通过官方网站（https://www.dfca.cn/）公布与其相关的信息。该网站是 DFCA 发布所有信息的最权威、最及时、最主要的渠道。网站发布的内容主要包括：

1. CPS、CP 的所有版本；
2. 证书链，包括：国家根证书、东方新诚信运营 CA 证书；
3. 证书信息、状态信息等查询服务；
4. 详细的业务办理指南，包括但不限于：服务网点地址、营业时间、联系电话等；
5. 依赖方协议；
6. 投诉处理政策及投诉方式，包括但不限于：投诉处理部门的地址、联系电话、电子邮件地址，以及内部监督部门名称。

2.2 信息发布方式

各类信息的发布方式如下：

1. CPS、CP 的所有版本：

(1) 网站提供下载链接

2. 证书链，包括：国家根证书、东方新诚信运营 CA 证书

(1) 网站提供下载链接

3. 证书信息、状态信息等查询服务

(1) 证书，通过 DFCA 的目录服务器发布。用户需使用相关工具访问目录服务器查询或下载证书；

(2) CRL，网站提供下载链接，或通过 DFCA 的目录服务器发布；

(3) 状态信息查询，网站提供专门页面对证书状态进行查询，并提供 OCSP 服务端口，用户可通过 OCSP 服务端口进行在线证书状态查询。

4. 详细的业务办理指南

(1) 网站提供下载链接

5. 依赖方协议

(1) 网站提供下载链接

6. 投诉处理政策及投诉方式

(1) 网站提供专门页面，显示投诉处理政策与投诉方式

2.3 监管备案

在 CPS 下载页面，声明 CPS 已经按照国家电子认证服务管理平台的要求进行了备案。

2.4 证书信息对接

DFCA 将根据主管机关的要求，及时完成与国家电子认证服务管理平台的技术对接，实现根据证书唯一编码、订户身份信息等维度查询 DFCA 已签发证书列表的功能

2.5 发布的时间与频率

1. CPS 的发布时间与频率

CPS 经 DFCA 审批通过后，将在正式生效后二个工作日内在门户网站上发布。

2. 证书/CRL 的发布时间与频率

(1) DFCA 的证书一经签发，在 1 小时内发布到 LDAP 服务器；

(2) DFCA 的 CRL 一经签发，在 1 小时内发布。CRL 每天更新发布一次；

(3) 通过 OCSP 对证书状态的查询是及时的。

3. 其他公告、通知等信息的发布时间与频率

(1) 根据实际业务开展的需要，DFCA 将在信息正式生效后二个工作日之内在门户网站正式发布；

(2) 这类信息是不定期发布的。

2.6 信息库访问控制

对于公布的本 CPS、证书、CRL 等信息，DFCA 允许公众自行通过网站和目录服务器

进行查询与访问。

DFCA 设置了访问控制与安全审计措施，保证只有经授权的 DFCA 业务人员才能编写和修改 DFCA 在线公布的信息。

3 身份标识与查验

3.1 身份查验通用要求

3.1.1 通用要求

DFCA 遵循《电子签名法》等法律法规与电子认证服务相关业务规范的要求，遵照本 CPS，面向客户提供证书的申请、延期、更新、冻结、解冻、撤销等业务。

在受理证书申请时，DFCA 将通过多种方式对订户和/或受托人进行业务告知、身份确认、意愿确认，并记录相关数据。客户与 DFCA 在业务申请表与电子认证服务协议上盖章或签字确认，视同协议签署。

DFCA 在进行身份查验时，身份查验义务未委托给外部机构或个人（非属同一法人主体的机构视为外部机构）。

3.1.2 订户告知

3.1.2.1 告知内容

DFCA 在订户申请证书时，向订户告知以下内容：

1. 订户的权利和义务；
2. 服务收费的项目和标准；
3. 电子签名认证证书、电子签名的使用条件；
4. 信息安全保障措施；
5. CA 和订户的责任划分；
6. 订户签名私钥的存储方式及安全要求；
7. 订户不得将所获证书用于任何违法违规、违背公序良俗，不得利用证书从事侵害国京利益、社会公共利益及第三方合法权益的活动。

3.1.2.2 告知方式

根据电子签名认证证书的类型不同，DFCA 采用不同的告知方式。

1. 对于个人高等级电子签名认证证书、机构高等级电子签名认证证书，可采用以下方式进行业务告知，并保留告知记录（包括告知方式、告知时间、告知内容等）：
   (1) 面对面；
   (2) 电话；
   (3) 视频；
   (4) 主管部门认可的其他方式。
2. 对于个人基础级电子签名认证证书、机构基础级电子签名认证证书，可采用以下方式进行业务告知，并保留告知记录（包括告知方式、告知时间、告知内容等）：
   (1) 采用高等级证书的告知方式告知；
   (2) 强制阅读；
   (3) 短信；
   (4) 邮件。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

订户签名密钥由订户密码设备生成。在证书请求信息中包含订户的签名公钥，以及对应的私钥生成的数字签名。DFCA 在签发证书时，使用订户的签名公钥验证证书请求信息中所包含的数字签名，来证明订户持有与公钥对应的私钥。

3.2.2 个人身份的查验

3.2.2.1 个人身份信息有效性的确认

DFCA 在受理个人证书申请时，需对订户或受托人的个人身份信息进行查验：

1. 受理个人证书申请时，应要求订户出示其有效身份证件或有效身份证件信息。可使用的有效身份证件为法律法规和国家有关文件规定的身份证件，包括但不限于：

(1) 居民身份证

(2) 港澳台居民居住证

(3) 港澳台居民来往内地通行证

(4) 护照

(5) 公安部居民身份证网上副本

(6) 公民网络身份标识（eID）

(7) 户口簿等

2. DFCA 采用以下方式查验订户身份证件的真实性和有效性：

(1) 通过公安主管部门认可的证件机读工具；

(2) 权威数据库；

(3) 主管部门认可的其他方式。

3. 当订户委托他人代为办理时，除前述核验订户的有效身份证件或有效身份证件信息外，还需同时查验订户本人签署的有效书面授权证明，并要求受托人出示其有效身份证件或有效身份证件信息，并按照上述 2 款方式查验订户和受托人的身份证件或身份资料。

DFCA 保留根据最新国家政策、法律、法规的要求更新个人身份信息有效性确认方式的权利。

3.2.2.2 个人高等级证书的实人查验

对于申请个人高等级证书的，需对订户开展实人查验。支持的实人查验的方式如下：

1. 面对面查验。由 DFCA 的业务人员对订户进行面对面的实人查验，适用于业务现场办理的情形；
2. 远程人工面对面查验。由 DFCA 的业务人员通过视频方式，对订户进行实人查验；
3. 生物特征验证。采用活体人脸、指纹、声纹、掌纹等生物识别技术，对订户进行实人查验；
4. 主管部门认可的其他方式。

DFCA 将以可追溯的方式完整记录并保存身份查验过程和结果，并保障记录数据的安全。每张证书申请，均建立独立的身份验证记录。

3.2.2.3 个人基础级证书的实人查验

对于申请个人基础级证书的，需对订户开展实人查验。支持的实人查验的方式如下：

1. 第 3.2.2.2 节规定的方式；
2. 电信运营商三要素查验，即核对“姓名、证件号码、手机号”在电信运营商的一致性，并通过对应手机号的随机短信验证码核验；
3. 银行卡四要素查验，即核对“姓名、证件号码、银行卡号、银行预留手机号”在银行的一致性，并通过预留手机号的随机短信验证码核验；
4. 申请人使用本人持有 DFCA 签发的有效电子签名认证证书对申请数据进行签名，DFCA 对签名数据进行签名验证；
5. 通过主管部门认可的其他方式：
   (1) 居民身份网络可信认证
   (2) 公民网络电子身份标识
   (3) 国家网络身份认证系统
   (4) 内地银行或支付机构对外提供的个人账户和身份信息对应关系验证等。

DFCA 将以可追溯的方式完整记录并保存身份查验过程和结果，并保障记录数据的安全。每张证书申请，均建立独立的身份验证记录。

3.2.3 机构身份的查验

3.2.3.1 机构身份信息有效性的确认

DFCA 在受理机构证书申请时，需对机构与受托人的身份信息进行查验：

1. 受理机构证书申请时，应要求受托人出示机构的有效身份证件或有效身份证件信息。有效的机构身份证件为法律法规和国家有关文件规定的证件，包括但不限于：
   (1) 营业执照
   (2) 统一社会信用代码证书
   (3) 事业单位法人证书
   (4) 社会团体法人登记证书
   (5) 民办非企业单位登记证书

(6) 基金会法人登记证书

(7) 外国企业常驻代表机构登记证等

2. DFCA 采用以下方式查验机构身份证件的真实性和有效性：

(1) 权威数据库；

(2) 主管部门认可的其他方式。

3. 除前述核验机构有效身份证件或有效身份证件信息外，根据经办人类型，对经办人进行身份查验：

(1) 对于经办人是法定代表人的，按 3.2.2 的要求对法定代表人有效身份证件或有效身份证件信息进行查验；

(2) 对于经办人不是法定代表人的，需查验机构法定代表人签署、单位盖章的有效书面授权证明，并按 3.2.2 的要求对受托人有效身份证件或有效身份证件信息进行查验。

DFCA 保留根据最新国家政策、法律、法规的要求更新机构身份信息有效性确认方式的权利。

3.2.3.2 机构高等级证书的实人查验

对于申请机构高等级证书的，需对经办人（法定代表人或受托人）开展实人查验。支持的实人查验的方式如下：

1. 对于经办人是法定代表人的，按 3.2.2.2 的查验方式开展实人查验；

2. 对于经办人是受托人的，除按 3.2.2.2 的查验方式开展实人查验外，还需通过机构对公账户随机金额打款进行验证或主管部门认可的其他方式。

DFCA 将以可追溯的方式完整记录并保存身份查验过程和结果，并保障记录数据的安全。每张证书申请，均建立独立的身份验证记录。

3.2.3.3 机构基础级证书的实人查验

对于申请机构基础级证书的，需对经办人（法定代表人或受托人）开展实人查验。支持的实人查验的方式如下：

1. 按 3.2.2.3 的查验方式，开展实人查验；

2. 订户使用 DFCA 签发的有效的 DFCA 的高等级机构证书对申请数据进行签名，DFCA 对签名数据进行验证。

DFCA 将以可追溯的方式完整记录并保存身份查验过程和结果，并保障记录数据的安全。每张证书申请，均建立独立的身份验证记录。

3.3 密钥更新请求的身份标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

证书常规密钥更新中，证书订户使用当前私钥对密钥更新请求进行签名，DFCA 使用订户原有公钥验证确认签名来进行订户身份标识和鉴别。DFCA 也可以使用初始身份确认相同的流程进行标识与鉴别。

3.3.2 撤销后密钥更新的标识与鉴别

证书撤销后的密钥更新等同于订户重新申请证书，其要求与本 CPS 的 3.2 相同。

3.3.3 证书变更的标识与鉴别

数字证书所载明的信息发生变化，订户应申请证书变更。订户通过原有私钥对变更请求进行签名，DFCA 使用订户原有公钥验证确认签名来进行订户身份标识与鉴别。

DFCA 保留要求订户按照证书新办提交申请材料的权利。

3.3.4 撤销请求的标识与鉴别

证书撤销请求的标识与鉴别使用初始身份验证相同的流程，其要求与本 CPS 的 3.2 相同。

如果是因为订户没有履行本 CPS 所规定的义务，由 DFCA 或其注册机构申请撤销订户的证书时，不需要对订户身份进行标识和鉴别。

3.4 订户意愿记录

3.4.1 订户意愿记录内容

在申请证书时，DFCA 需向订户明确展示以下内容：

1. 订户身份信息；
2. CA 的信息；
3. 签名私钥保存方及其保存义务；
4. 订户对电子签名的法律责任。

订户应明确表示对上述 1 至 4 项内容已充分知晓并同意。

3.4.2 个人高等级证书的意愿记录

对于个人高等级证书，根据证书申请的办理模式，订户意愿的确认方式规定如下。

1. 现场办理时，采用以下方式进行订户意愿的确认，并采用录音录像或通过主管部门认可的其他方式记录订户意愿：
   (1) 面对面确认；
   (2) 手抄提示语。
2. 远程或在线办理时，采用以下方式进行订户意愿的确认，并采用录音录像或通过主管部门认可的其他方式记录订户意愿：
   (1) 音视频；
   (2) 主管部门认可的其他方式。

3.4.3 个人基础级证书的意愿记录

对于个人基础级证书，采用下列方式之一进行订户意愿的确认，并保留完整、可追溯的订户意愿记录：

1. 按 3.4.2 的要求确认并记录订户意愿；
2. 显示意愿记录内容，强制订户阅读的方式。

3.4.4 机构高等级证书的意愿记录

对于机构高等级证书，根据经办人的不同，采用下列方式之一进行订户意愿的确认，并采用录音录像或通过主管部门认可的其他方式记录订户意愿：

1. 对于经办人是法定代表人的，按照 3.4.2 的方式确认机构法定代表人的意愿；
2. 对于经办人是受托人的，查验法定代表人签署、加盖机构公章的授权文件，并按照 3.4.2 的方式确认受托人的意愿。

3.4.5 机构基础级证书的意愿记录

对于机构基础级证书，根据经办人的不同，采用下列方式之一进行订户意愿的确认，并保留完整、可追溯的订户意愿记录：

1. 对于经办人是法定代表人的，按照 3.4.3 的方式确认机构法定代表人的意愿；
2. 对于经办人是受托人的，查验法定代表人签署、加盖机构公章的授权文件，并按照 3.4.3 的方式确认受托人的意愿。

3.5 订户协议

订户在申请证书时，应与 DFCA 签署订户协议。订户协议内容包含 3.1.2.1 中规定的内容。

3.6 未验证的订户信息

除该类型证书所必须要求的身份信息需要得到明确、可靠的验证以外，DFCA 不对申请时的其他信息予以验证。

对于没有验证过的订户信息，DFCA 将不承诺此类信息的真实性，并且在所签发的证书中不包含未经验证的订户信息。

3.7 互操作要求

在互操作业务情形中，DFCA 的义务与责任主要包括：

1. 信任准入义务

(1) 审慎审核对接方 CA 资质、认证资质、安全体系，不合规不予互认；

(2) 明确互操作信任边界、采信范围、证书适用业务场景。

2. 证书核验责任

(1) 对外部接入证书做合法性、有效期、撤销状态校验；

(2) 拒绝无效、撤销、篡改、超出采信范围的外部证书。

3. 信息同步与发布义务

(1) 同步互认 CA 根证书、中级证书信息；

(2) 正常推送 CRL、OCSP 撤销数据，保障跨域状态查询可用。

4. 安全风控责任

(1) 制定跨域风险处置规则，防范伪造、冒用、证书攻击；

(2) 出现异常证书风险，及时预警、暂停互认、追溯排查。

5. 业务合规与告知义务

(1) 按法律法规、电子认证规范开展互操作；

(2) 向证书用户明确跨机构采信范围、使用限制、风险提示。

6. 纠纷与追责责任

(1) 界定跨 CA 间权责划分，明确差错、侵权、事故责任归属；

(2) 配合对方 CA 开展核查、溯源、取证、善后处理。

7. 互认变更终止义务

(3) 互认关系调整、暂停、终止时，提前公示告知；

(4) 妥善处理存量跨域证书业务平稳过渡。

目前，DFCA 未开展与其他 CA 的互操作业务。

3.8 命名

在 DFCA 证书服务体系中，主体甄别名称（以下简称“DN”）不是唯一的。DFCA 所签发的电子签名认证证书的主体甄别名称（以下简称“DN”）结构定义符合 GB/T 16264.8 的要求，DN 项编码规则见表 3-1。

表 3-1 证书主体 DN 项代码

代码	说明	示例
C	国家	CN
S	省份（可选）	湖南

L	城市（可选）	长沙
O	订户所在机构信息（可选）	xx 公司
OU	订户所在机构部门信息（可选）	xx 部门
CN	订户名称（个人姓名或机构法定名称）	张三/xx 公司/xx 公司 xx 部门

根据证书类型不同，DN 的命名规则如下：

1. 对于个人证书，证书主体甄别名称的命名规则如下：
   (1) 不允许和不接受任何匿名或伪名。甄别名必须具有明确的、肯定的意义，能够与证书主体所对应的个人建立确定联系；
   (2) 甄别名应当符合法律法规等相关规定的要求；
   (3) 签发的证书不包含任何商标或者可能对其他机构构成侵权的信息；
   (4) DN 项中 CN，由订户在申请时指定，可为订户的姓名，或在相关业务系统的用户名；
   (5) 在证书扩展项中包含由姓名、身份证件类型、身份证件号码组成的信息的散列值；
   (6) 根据应用需要，在证书扩展项可增加应用所需的订户身份的其他内容。
2. 对于机构证书，证书主体甄别名称的命名规则如下：
   (1) 不允许和不接受任何匿名或伪名。甄别名必须具有明确的、肯定的意义，能够与证书主体所对应的机构建立确定联系；
   (2) 甄别名应当符合法律法规等相关规定的要求；
   (3) 主体 DN 项中包含机构名称；
   (4) 在证书扩展项中包含组织机构的有效证件类型及其编号；
   (5) 签发的证书不包含任何商标或者可能对其他机构构成侵权的信息；
   (6) 根据应用需要，在证书扩展项可增加应用所需的订户身份的其他内容。

4 证书生存周期操作要求

4.1 通用要求

在证书生存周期的各项操作过程中，DFCA 与各方应切实履行自身责任。

1. DFCA 的责任，主要包括但不限于：
   (1) 承担建立运营和维护注册通道的责任；
   (2) 承担与订户签订电子认证服务协议的责任；
   (3) 明确证书生存周期操作的办理流程（各证书业务申请流程见本章后续相关章节内容）；
   (4) 承担妥善记录并保存相关信息的责任；
   (5) 按照本 CPS 的规定对订户申请办理证书生存周期业务进行身份确认、意愿确认。
2. 订户的责任，主要包括但不限于：
   (1) 承担提供准确、真实、有效信息的责任；
   (2) 按照本 CPS 的流程要求，申请办理证书生存周期业务；
   (3) 配合 DFCA 完成证书生存周期业务相关的身份确认、意愿确认；
   (4) 与 DFCA 签署服务协议；
   (5) 按本 CPS 要求，使用证书与保管密钥。

4.2 证书申请

4.2.1 证书申请实体

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

4.2.2 证书申请流程与责任

订户按照本 CPS 所规定的要求，通过现场面对面或在线方式提交证书申请，包括相关的身份证明材料。

DFCA 或其注册机构按 3.1.2 的要求，明确告知订户相关内容，并保存告知记录。

DFCA 或其注册机构按 3.4 的要求，确认订户意愿，并保存订户意愿记录。

在订户表达申请证书的意愿后，DFCA 或其注册机构按 3.2 的初始身份确认的要求，对订户的身份进行鉴别，并决定是否受理申请。

订户需要提供本 CPS 的 3.2 所述的有效身份证明材料，并确保材料真实准确。配合 CA 机构或其注册机构完成对告知内容确认、申请意愿身份信息的采集、记录和审核。如订户未向 CA 机构提供真实、完整和准确的信息，或者有其他过错，给 CA 机构或电子签名依赖方造成损失的，由订户承担赔偿责任。

DFCA 参照本 CPS § 3.2 的要求对订户的身份信息进行采集、记录，审核。通过鉴证后，DFCA 向订户签发证书。如果用户身份信息的鉴别由其注册机构完成，CA 机构应对其注册机构进行监督管理和审计。

订户应当提供真实、完整和准确的信息，CA 机构或其注册机构须按本 CPS § 3.2 的要求和流程对订户身份材料信息进行审查。

4.3 证书申请处理

4.3.1 执行身份确认功能

DFCA 或其注册机构按照本 CPS 的 3.2 所规定的身份确认流程对订户的身份进行确认。

4.3.2 证书申请批准和拒绝

DFCA 或其注册机构根据本 CPS 所规定的身份确认流程对订户身份进行确认后，根据身份确认结果决定批准或拒绝证书申请。

如果订户通过本 CPS 所规定的身份确认流程且鉴证结果为通过，DFCA 或其注册机构将批准证书申请，为订户签发数字证书。

订户未能通过身份确认的，DFCA 或其注册机构将拒绝订户的证书申请，并通知订户证

书申请鉴证失败，同时向订户提供失败的原因（法律禁止的除外）。

被拒绝的订户可以在准备正确的材料后，重新提出申请。

在必要时 DFCA 有权复核注册机构提交的订户申请材料，并有权拒绝不符合本 CPS 的高风险申请。

DFCA 或其注册机构能否在上述时间期限内处理证书申请取决于订户是否真实、完整、准确地提交了相关信息和是否及时地响应了 DFCA 或其注册机构的管理要求。

在证书申请被审核通过或拒绝前，订户可主动撤销本次申请。订户在此之前所提交的申请材料，DFCA 或其注册机构不予退回。

4.3.3 证书申请处理时限

DFCA或其注册机构在收到了所有必须的相关信息后，将在2个工作日内处理证书申请。因特殊情况确需超期的（例如，因物流原因，导致申请材料无法按时送达等），DFCA 的工作人员将与订户协商确定处理时限。

4.4 证书签发

4.4.1 证书签发过程中 DFCA 的行为

DFCA 在批准证书申请后，根据证书申请数据签发数字证书。证书的签发意味着 DFCA 最终完全正式地批准了证书申请。

DFCA 建设了安全的证书签发系统，制定了严格的管理流程，从技术与管理上保证了证书签发的安全。

在签发证书时，与该证书相对应的私钥只存放在用户密码设备（例如，智能密码钥匙等通过国家密码主管部门安全性审查的硬件密码设备）内，不会留存任何备份（加密密钥除外）；同时，证书签发系统验证证书申请数据的签名数据，以确认用户拥有与证书申请中公钥所对应的私钥。证书签发系统将加密密钥对使用证书申请的签名公钥进行加密保护，确保只有订户才能导入对应的加密密钥对。

当订户申领证书时，由 DFCA 或其注册机构对其身份进行确认与审核，并将证书与订户进行绑定，该证书才能被订户有效使用。

4.4.2 结果通告

DFCA 对于证书申请的处理结果，采用以下方式向订户通告：

1. 面对面的方式：DFCA 或其注册机构现场完成证书的制作，当面通知交交付给订户；
2. 站内消息：在业务网站，通过站内消息通知订户；
3. 电子邮件方式：发送通知至订户或受托人的电子邮箱；
4. 主管部门认可的方式；
5. 其他 DFCA 认为安全可行的方式。

4.5 证书接受

4.5.1 构成接受证书的行为

订户接受证书可以通过以下方式：

1. DFCA 或其注册机构将数字证书当面或寄送交付订户。订户从获得数字证书起，就视为已经接受证书；
2. 对于订户通过网站下载证书的，订户完成证书的下载，表明订户已经接受证书；
3. 从订户将证书应用于对应的电子签名或其他密码运算时起，就视为已经接受证书；
4. 主管部门认可的方式；
5. DFCA 也可以通过其他安全的方式交付数字证书；

DFCA 保存订户接受证书的记录，包括接受时间、方式、操作人等信息。

4.5.2 证书的发布

DFCA 在签发完数字证书后，存储在系统的数据库中，并同步发布到主目录服务器。主目录服务器与从目录服务器，通过同步模式，实现证书数据同步。当证书同步至从目录服务器，DFCA 即完成了证书的发布。

对已发布的数字证书，DFCA 提供以下证书信息查询服务。

1. 目录服务：用户通过访问 DFCA 的从目录服务器，可以查询下载相关的证书与 CRL；
2. OCSP 服务：用户通过访问 DFCA 的 OCSP 服务，可以实时查询证书的状态；
3. 网站查询：用户在网站上输入查询条件，可查询对应的证书。

4.5.3 在颁发证书时对其他实体的通告

一般情况下，DFCA 不需要将证书签发情况通知其他实体，其他实体可以通过 DFCA 提供的查询方式自行查询。根据应用，DFCA 可采取以下方式对其他实体进行通知：

1. 定时推送：DFCA 将证书定时推送到对应的应用系统；
2. 接口查询：DFCA 提供证书查询接口，接收应用系统的查询，返回对应的数字证书信息。

4.6 密钥对和证书的使用

4.6.1 密钥对的安全保护

在将密钥对交付订户保管之前，CA 采取必要的有效措施保障其安全性，包括但不限于：

1. 签名私钥的保护：
   (1) 使用国家密码主管部门批准的密码设备（例如，智能密码钥匙等）生成签名私钥；
   (2) 签名私钥不可明文导出设备。
2. 加密私钥的保护：
   (1) 使用国家密码主管部门批准的密钥管理系统、密码设备，生成用户的加密密钥对；
   (2) 加密密钥对加密保存在系统数据库中；
   (3) 使用用户的签名公钥对加密私钥进行加密保护；
   (4) 加密私钥以密文方式导入用户的密码设备。
3. 安全事件反馈：DFCA 提供电话热线，支持外部安全事件反馈，及时受理和处理证书信息错误、私钥失密或证书被盗用等情况；
4. 目前，DFCA 只支持使用 SM2、SM3、SM4 密码算法；
5. 目前，DFCA 不提供私钥管理服务。

4.6.2 订户对私钥和证书的使用

订户在提交了证书申请并接受了 DFCA 所签发的证书后，均视为已经同意遵守与

DFCA、依赖方有关的权利和义务的条款。

订户接受数字证书后，应妥善保存其证书对应的私钥。

订户只能在指定的应用范围内使用私钥和证书，订户只有在接受了相关证书之后才能使用对应的私钥，并且在证书到期或被撤销之后，订户必须停止使用该证书对应的私钥。

4.6.3 依赖方对公钥和证书的使用

依赖方只能在指定的应用范围内依赖于证书，并且与证书要求相一致（如，证书等级、密钥用途扩展等）。依赖方获得对方的证书和公钥后，可以通过查看对方的证书了解对方的身份，并通过公钥验证对方电子签名的真实性。依赖方查看证书了解对方的身份时，应查看该证书的甄别名、内容、证书策略，对应本 CPS 的 3.2 定义的不同的鉴别方法，选择是否信任证书中标识的身份，承担不同鉴别方法可能存在的风险。

数字证书的有效性验证，包括以下方面的验证：

1. 证书签名验证：使用 DFCA 的运营 CA 证书验证用户数字证书中的签名，确认该证书是 DFCA 签发的，并且证书的内容没有被篡改；
2. 有效期验证：检验证书的有效期，确认该证书在有效期之内；
3. 证书状态验证：通过 CRL 或 OCSP，检查证书状态，确认没有被撤销。

在验证电子签名时，依赖方应准确知道什么数据已被签名。在公钥密码标准里，标准的签名信息格式被用来准确表示签名过的数据。

4.7 证书续期

4.7.1 证书续期更新的情形

证书续期是指在不改变订户主体信息的情况下，在原证书到期前，为订户签发新证书。

证书续期的具体情形如下：

1. 证书有效期将要到期；
2. 希望延长证书有效期。

4.7.2 证书续期的申请主体

证书续期的申请主体，应为订户或其受托人。

4.7.3 证书续期的申请处理

DFCA 对于证书续期请求时的身份查验，采用以下规则：

1. 若自申请人上次完成身份查验之日起至本次续期申请日未满三年（申请人为原证书的申请人），可使用有效的原证书进行电子签名验证的方式进行确认；
2. 否则，按照 3.2 的规定，重新对申请人进行身份查验。

4.7.4 证书签发与接受

证书签发与接受的流程，遵照本 CPS 的 4.4 与 4.5 的规定。

4.8 证书密钥更新

4.8.1 证书密钥更新的情形

证书密钥更新是指在证书到期前，在不改变订户主体信息的情况下，为订户生成新的密钥对，并签发新证书。

证书密钥更新的具体情形如下：

1. 因私钥泄漏而撤销证书；
2. 证书无法继续获得信任；
3. 证书无法正常使用，例如，证书载体损坏；
4. 证书丢失；
5. 其他需要更新证书密钥的情形。

4.8.2 证书密钥更新的申请主体

证书密钥更新的申请主体，应为订户或其受托人。

4.8.3 证书密钥更新的申请处理

DFCA 对于证书密钥更新请求时的身份查验，采用以下规则：

1. 若自申请人上次完成身份查验之日起至本次密钥更新申请日未满三年（申请人为原证书的申请人），可使用有效的原证书（若可用）进行电子签名验证的方式进行确认；
2. 否则，按照 3.2 的规定，重新对申请人进行身份查验。

4.8.4 证书签发与接受

证书签发与接受的流程，遵照本 CPS 的 4.4 与 4.5 的规定。

4.9 证书变更

4.9.1 证书变更的情形

证书变更是指在证书到期前，在不改变证书的公钥和有效终止期的情况下，为订户签发新证书。

证书变更的具体情形如下：

1. 除订户的唯一身份标识外的身份信息改变，例如，订户名称；
2. 其他需要变更证书的情形。

4.9.2 证书变更的申请主体

证书变更的申请主体，应为订户或其受托人。

4.9.3 证书变更的申请处理

DFCA 对于证书变更请求时的身份查验，采用以下规则：

1. 若自申请人上次完成身份查验之日起至本次变更申请日未满三年（申请人为原证书的申请人），可使用有效的原证书（若可用）进行电子签名验证的方式进行确认；
2. 否则，按照 3.2 的规定，重新对申请人进行身份查验。

4.9.4 证书签发与接受

证书签发与接受的流程，遵照本 CPS 的 4.4 与 4.5 的规定。

4.10 证书撤销或冻结

4.10.1 证书撤销或冻结的情形

证书撤销是指在证书到期前，需要停止使用证书。

证书撤销的具体情形如下：

1. 发生下列情形之一的，订户应当申请撤销数字证书：
   (1) 私钥泄露；
   (2) 数字证书中的信息发生重大变更；
   (3) 认为本人不能实际履行本 CPS；
   (4) 认为当前密钥管理方式的安全性得不到保证。
2. 发生下列情形之一的，CA 机构可以强制撤销其签发的数字证书：
   (1) 订户提供的信息不真实；
   (2) 订户没有履行双方合同规定的义务，或违反本 CPS；
   (3) 数字证书的安全性得不到保证；
   (4) 法律、行政法规规定的其他情形。

4.10.2 证书撤销或冻结的申请主体

证书撤销或冻结的申请主体，分为以下两种情况：

1. 订户或其受托人；
2. DFCA 或其注册机构。

4.10.3 证书撤销或冻结的申请处理

4.10.3.1 订户撤销申请

证书撤销请求的处理，采用与证书签发相似的流程

1. DFCA 提供热线电话、业务网站等证书撤销申请渠道，记录影响证书或私钥安全的事件（如密钥遗失、泄露）；
2. 证书撤销或冻结的申请人，通过在线方式或离线方式发起撤销申请，并注明撤销或冻结原因；
3. DFCA 或其注册机构根据本 CPS 的 3.2 的要求，对订户提交的撤销或冻结请求进行身份查验与审核，以确认为订户本人或得到了订户的授权；
4. DFCA 撤销或冻结订户证书后，DFCA 或其注册机构将通知订户证书被撤销或冻结，订户的数字证书在 24 小时内进入 CRL，向外界发布。

DFCA 按照证书申请的要求，保留订户撤销申请的处理过程与相关信息。

4.10.3.2 强制注销申请

强制注销是指当 DFCA 或其注册机构确认订户有违反本 CPS 的情况发生时，对订户证书进行强制注销，注销后将通知该订户。

DFCA 保留证书强制撤销的处理过程与相关信息。

4.10.4 注销请求宽限期

如果出现私钥泄露等事件，注销和冻结请求必须在发现泄露或有泄露嫌疑 8 小时内提

出。其他注销和冻结原因的注销请求必须在 48 小时内提出。

4.10.5 DFCA 处理注销请求的时限

DFCA 接到注销/冻结请求后实时处理，24 小时生效。

DFCA 每日签发一次 CRL，并将最新的 CRL 发布到证书服务系统的目录服务器，供订户和依赖方查询下载。

4.10.6 依赖方检查证书注销的要求

依赖方应验证 CRL 的可靠性和完整性，确保是经 DFCA 发布并且签名的。依赖方可以使用以下两种方式查询所依赖证书的证书状态：

1. CRL 查询：通过目录服务器提供的查询系统，查询并下载 CRL 到本地，进行证书状态的检验；
2. 在线证书状态查询（OCSP）：DFCA 接受证书状态查询请求，查询证书的实时状态。查询结果经过签名后，返回给请求者。

4.10.7 CRL 发布频率

CRL 的发布周期为 24 小时，即每日发布一次 CRL。

4.10.8 CRL 发布的最大滞后时间

发布的最长滞后时间为 24 小时。

4.10.9 ARL 发布频率

DFCA 目前未发布 ARL。

4.11 证书状态信息服务

4.11.1 证书状态信息服务方式

DFCA 向订户和依赖方提供在线证书状态查询服务（OCSP 服务），OCSP 服务地址为：www.dfca.cn:2415。

4.11.2 证书状态信息服务的可用性

OCSP 服务响应时间不大于 5 秒。

DFCA 提供 7×24 小时的 OCSP 查询服务，服务可用率不低于 99%。

4.11.3 备用服务

根据请求者的要求，在支付相关费用后，DFCA 支持提供以下备用的证书状态信息服务：

1. 收到证书主题的电子签名消息的接受者要求，确认该证书是否已被撤销；
2. 提供通知服务，当指定的证书被撤销时，CA 机构将通知请求该项服务的请求者。

4.12 停止使用认证服务

4.12.1 停止使用认证服务的情形

停止使用认证服务是指当证书有效期满或证书注销后，该证书的服务时间结束。

下列情况视为证书持有者终止使用 DFCA 提供的认证服务：

1. 证书到期后，订户不再延长证书使用期或者不再重新申请证书，则可以自动终止与 DFCA 的服务；
2. 在证书有效期内，订户提出终止服务，即服务终止。

4.12.2 停止使用认证服务的处理

1. 处理时限与方式：

   (1) 对于证书到期后的认证服务停止，DFCA 无须任何处理；

(2) 对于有效期内订提出终止服务的（暨提出证书撤销申请的），DFCA 按 4.10.5 的要求完成证书撤销处理。

2. 用户数据处理：

(1) 用户数据，包括“申请数据、证书数据”等；

(2) 停止认证服务后的用户数据处理，按数据归档管理进行处理。

3. 停止服务后，将可能涉及的责任延续条款以邮件方式通知订户。主要的责任延续条款主要包括：

(1) 证书停用生效责任：提交申请后，配合完成证书撤销、冻结，不再使用该证书进行电子签名、数据加密等业务；

(2) 历史行为追责延续：服务终止前使用证书产生的签章、交易、协议效力、法律权责依旧有效，相关责任不予免除；

(3) 涉密数据保密义务：继续保密业务资料、密钥信息、往来数据，不得外泄滥用；

(4) 费用结清责任：按协议结清存续周期服务费、违约金、相关损耗费用；

(5) 配合核查举证责任：后续涉纠纷、审计、案件调查，须配合取证核验历史证书使用记录；

(6) 第三方关联权责：终止前绑定的业务系统、合作对接权限，自行办理解除，承担解绑相关后果；

(7) 违规过错兜底责任：终止服务前发生的冒用、违约、侵权行为，仍需承担对应法律与民事责任；

(8) 密钥销毁保管义务：妥善处置密钥载体，防止私钥泄露、二次冒用风险。

4.13 密钥托管与恢复

4.13.1 密钥托管与恢复概述

DFCA 的运营 CA 证书私钥，存储在 DFCA 自身的屏蔽机房的密码设备内，不得托管给任何第三方机构或个人。

DFCA 建立了运营 CA 证书密钥备份与恢复策略，对根证书密钥进行安全备份。

具体策略在“6.1 密钥生成与安装”与“6.2 私钥的安全保证”中详细描述。

4.13.2 密钥托管与恢复的策略与行为

订户的签名密钥对由订户的密码设备生成，或由密码设备与经国家认证的第三方密钥服务机构生成，加密密钥对由密钥管理中心生成。

具体策略在“6.1 密钥生成与安装”与“6.2 私钥的安全保证”中详细描述。

4.13.3 密钥托管与恢复的策略与行为

4.13.3.1 密钥托管策略与行为

签名密钥对由订户的密码设备保管，加密密钥对由订户的密码设备保管；同时，密钥管理中心保存有加密密钥对的备份数据，以便于密钥恢复。

4.13.3.2 密钥恢复策略与行为

密钥恢复是指加密密钥对的恢复，DFCA 不负责签名密钥对的恢复。

密钥恢复分为两类：订户密钥恢复和司法取证密钥恢复：

1. 订户密钥恢复

当订户的密钥损坏或丢失后，某些密文数据将无法还原，此时订户可申请密钥恢复。订户向 DFCA 申请进行密钥恢复。经审核后，通过 DFCA 向密钥管理中心请求密钥恢复；密钥管理中心接受订户的恢复请求，恢复订户的密钥并下载于订户证书载体中。

2. 司法取证密钥恢复

司法取证人员向 DFCA 申请。由 DFCA 的业务人员根据司法机关的书面材料，生成司法取证密钥恢复申请。经审核后，由密钥管理中心恢复所需的密钥并记录于特定载体中。

4.13.4 会话密钥的封装与恢复的策略与行为

会话密钥的封装采用数字信封的方式。数字信封使用接收者的公钥对会话密钥加密，接收者用自己的私钥解密，恢复会话密钥。

5 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

DFCA 的建筑物和机房建设按照下列标准实施：

1. GB 50174-2008：《电子计算机机房设计规范》
2. GB 2887-2000：《电子计算机场地通用规范》
3. GB 9361-88：《计算站场地安全要求》
4. SJ/T 10796-2001：《防静电活动地板通用规范》
5. GB 50034-2004：《建筑照明设计标准》
6. GB 50054-95：《低压配电设计规范》
7. GB 50019-2003：《采暖通风与空气调节设计规范》
8. GB 157：《建筑防雷设计规范》
9. GBJ 79-1985：《工业企业通信接地设计规范》

DFCA 机房位于长沙麓谷高新区标志麓谷坐标 A 栋 1502，实行分区访问的安全管理：

DFCA 机房的功能区域划分为 CA 核心区、CA 管理区、CA 服务区、RA 管理区与监控管理区等区域。

CA 核心区位于屏蔽机房内，具有最高的安全级别。屏蔽机房设置了非接触 IC 卡指纹门禁系统，并设置了“双人同进、双人同出”策略，即需要两个持有相应 IC 卡的管理人员同时刷卡，方可进入该区域。

其它区域的进入权限授权给不同的管理人员，不能有一个管理人员可单独进入多个区域的情况。

物理访问信息记录在门禁系统中，定时导出保存到公司档案室。

5.1.2 门禁与监控

为了保证 CA 系统的安全，采取了一定的隔离、控制、监控手段。机房的所有门都足够结实，能防止非法的进入。机房通过设置门禁和侵入报警系统来重点保护机房物理安全。

物理访问控制包括如下几个方面：

1. 门禁系统:控制各层门的进出。工作人员需使用身份识别卡结合指纹鉴定才能进出，系统记录进出时间记录和信息提示。
2. 报警系统：当发生任何非法闯入、非正常手段的开门、长时间不关门等异常情况，均会触发报警系统。
3. 监控系统：部署有视频监控系统，对于屏蔽机房区域，进行 24 小时不间断录像，对于其他机房区域，采用动态录像方式进行监控。系统保留录像资料，以备查询。
4. 门禁访问记录的保存时间为 1 年，视频监控记录的保存时间这 3 个月。在上述记录在销毁前，DFCA 进行安全审计，形成的审计报告存档备查。

5.1.3 电力与空调

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统。按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备分开供电。供电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。计算机设备专用配电柜和辅助设备配电柜独立设置。

目前，DFCA 采用使用不间断电源系统（UPS）来保证供电的稳定性和可靠性，当市电停电时，维持系统正常运转。DFCA 的市电由高开区的市电接入供电。高开区的市电具有双市电供电，在第一路市电停电的情况下，将自动切换到第二路市电供电，维持系统正常运转。

DFCA 对 CA 系统的电源、空调等物理要求，严格参照相关设施管理的规定进行维护和保养，而且每年对其是否符合要求进行检查。

5.1.4 灾难备份

DFCA 尚未建立异地灾备系统。对于系统的根密钥等重要数据，租赁了银行保险箱，进行异地备份。

DFCA 定期进行数据备份并导出备份数据，与系统分开保存。

5.1.5 环境保障

根据机房环境及设计规范要求，机房内设置了空气调节系统。空气调节系统包括空调、通风管路，保持相对湿度在 40%-60%范围内，保持温度在 18-28C 范围内

机房内无渗水、漏水现象，主要设备采用专用的防水插座，并采取必要措施防止下雨或水管破损，造成天花板漏水、地板渗水和空调漏水等现象。

DFCA 的系统有充分保障，能够防止水侵蚀。

5.1.6 消防措施

火灾预防与保护措施主要包括以下六个方面：

1. 敏感区、高度敏感区域，其建筑物的耐火等级必须符合 GB 50045-1995《高层民用建筑设计防火规范》中规定的二级耐火等级；
2. DFCA 的设施内设置火灾报警装置。在机房内、各物理区域内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位设置烟、温感探测器；
3. 敏感区及高敏区配置独立的气体灭火装置，使用专业的灭火系统，备有相应的气体灭火器。DFCA 内除对纸介质等易燃物质进行灭火外，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂；
4. 火灾自动报警、自动灭火系统避开可能招致电磁干扰的区域或设备，同时配套设置消防控制室。还设有不间断的专用消防电源和直流备用电源，并具有自动和手动两种触发装置；
5. 在非敏感区及敏感区的办公区域内，设置紧急出口，紧急出口必须设有消防门，消防门符合安全要求。紧急出口门需与门禁报警设备联动。

灭火系统采用电动，手动，紧急启动三种方式：

1. 电动方式：防护区报警系统第一次火警确认后，发出声光警示信号，切断非消防电源（如：空调电源、照明电源等）。并送排风（烟），防火阀关闭。第二次火警确认后，经延时，同时发出气体释放信号，并发出启动电信号，送给对应的管网启动钢瓶，喷气灭火；
2. 手动方式：人员对钢瓶或药剂瓶直接开启操作；
3. 紧急启动：防护区外设有紧急启动按钮供紧急时使用。

DFCA 通过与专业防火部门协调，实施消防灭火等应急响应措施。

5.1.7 设备管理

DFCA 建立机房内所有设备的台账数据。台账数据包含每台设备的名称、品牌型号、配置、责任人、使用状态、维护周期和报废标准。

DFCA 定期进行设备盘点和核对，设备实际情况与设备台账相符。

5.1.8 存储介质管理

DFCA 制定了《信息系统介质保密管理制度》、《移动存储设备安全管理办法》等管理制度，明确规定存储介质的使用权限、报废标准、销毁方法和审批流程，完整记录存储媒体领用、归还、报废等情况，以加强存储介质的管理。

存储介质主要包括硬盘、软盘、磁带、光盘等。介质存储地点和系统分开并且保证物理安全，注意防磁、防静电干扰、防火、防水，由专人管理。

5.1.9 废物处理

当 DFCA 存档的敏感数据或密钥已不再需要或存档期限已满时，应当将这些数据进行销毁。写在纸张之上的，必须切碎或烧毁。如果保存在磁盘中，应多次重写覆盖磁盘的存储区域，其他介质以不可恢复原则进行相应的销毁处理。

5.2 操作过程控制

5.2.1 可信角色

DFCA 或其注册机构等组织中与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，必须由可信人员担任。

DFCA 明确规定 CA 关键职能的职位，主要包括但不限于以下部分：

1. 安全策略委员会主任：安全策略委员会的负责人，主持安全策略委员会的日常工作；
2. 可信人员管理员：负责 DFCA 的人员招聘、培训、考核等人事工作；
3. 安全管理员：负责 DFCA 的安全管理工作；
4. 密钥管理员：负责 CA 系统的根密钥、系统密钥等密钥数据的生成、备份、恢复等密钥管理工作；
5. 物理环境管理员：负责物理环境及相关设施的安全管理；
6. 技术运维人员：负责 CA 系统的服务器、网络等设备的日常运行与维护；
7. 数据库管理员：负责数据库进行日常运维、性能优化及数据备份等；
8. 系统管理员：负责 CA 系统的系统策略配置、用户与权限管理等日常运行与管理工作；
9. 系统审计员，负责系统和网络日志的审计、管理、审计报告生成等；
10. 运行审计管理员：负责对客户签发、客户服务等核心业务进行独立审计等；
11. 业务操作员：负责证书申请的受理、审核，订户的身份与意愿鉴证；
12. 客户档案管理员：负责客户证书相关档案资料的归档与保密等；
13. 其他人员：对公司运营有重要影响的其他管理人员，包括：财务、法务等。

DFCA 根据《电子认证服务机构从业人员岗位技能规范》等标准规范与本 CPS 的要求，规范证书服务机构和服务系统的管理人员、操作人员的岗位职责和操作行为。

5.2.2 职责分离

DFCA 对与运行和操作相关的职能有明确的分工，贯彻职责分割、多人控制、互相牵制、互相监督和最小权益的安全管理原则，所有涉及关键操作（密钥管理、审计、鉴证、系统管理）的角色应实现双人操作或复核机制；涉及业务连续性相关操作（运维、鉴证、审计等）

的角色按工作量设置人员冗余。在任何一人缺岗时仍能实现双人操作；禁止同一人员掌握可独立完成“发起、审批、执行、审计”全流程的任何组合，确保由多名可信人员共同完成敏感操作。有关职责分离的要求如下：

1. 访问和管理 CA 的加密设备及密钥，至少需要 3 个可信人员。
2. 对于证书申请的鉴别和签发，需要 3 个可信人员操作完成。
3. 对于重要的系统操作与维护，DFCA 通常会安排一人进行操作，一人进行监督记录。

5.2.3 每个角色的识别与鉴别

所有 DFCA 的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡和指纹识别；进入系统需要使用数字证书进行身份鉴别。DFCA 将独立完整地记录其所有的操作行为。

5.2.4 需要职责分割的角色

需要进行职责分割的角色，包括但不限于下列人员：

1. 系统管理员、技术运维员、数据库管理员、系统审计员之间不得兼任；
2. 同一证书业务的录入与审核环节不得由同一业务操作员完成；
3. 业务操作员、客户档案管理员、运营审计员之间不得兼任；
4. 密钥管理员不得与系统管理员、技术运维人员兼任；
5. 密钥管理员不与除安全策略委员会成员外的其他可信和角色兼任。

5.3 人员控制

5.3.1 可信人员资格要求

所有的员工与 DFCA 签订劳动合同与保密协议。对于充当可信角色或其他重要角色的人员，必须具备的一定的资格，具体要求在人事管理制度中规定。

DFCA 对于任职可信角色的人员的要求如下：

1. 从业经历调查要求和无犯罪记录；

2. 具备履行岗位职责所必需的专业技能要求；
3. 签署具有法律约束力的保密协议，承诺不得私自保存、复制或泄露电子认证服务的所有秘密或敏感信息；
4. 签署劳动合同；
5. 必须具备忠诚、可信赖及工作的热诚度、无影响 DFCA 运行的其它兼职工作等。

5.3.2 可信人员培训要求

DFCA 建立覆盖所有可信和角色的持续培训体系，对所有人员按照其岗位和角色安排不同的培训。具体要求包括：

1. 岗前培训：所有可信人员上岗前须完成不少于 20 学时的培训并通过考核；
2. 持续培训：每年至少接受一次培训，每人每年培训时长不少于 20 学时，并通过考核；
3. 培训内容主要包括但不限于：
   (1) 电子认证服务相关法律法规与标准；
   (2) 岗位通用职责要求及各角色特定的工作要求；
   (3) 内部管理政策、制度及流程等；
   (4) PKI 和密码技术基础知识；
   (5) CPS、CP；
   (6) 安全管理策略和机制；
   (7) DFCA 的安全原则和机制、岗位职责；
   (8) 电子认证系统相关软、硬件的安装与维护；
   (9) 电子认证系统的操作与使用；
   (10) DFCA 的业务管理相关的流程、标准与规范，包括订户身份查验与审核的策略和流程等；
   (11) DFCA 的运行管理相关的规章、制度与管理办法；
   (12) DFCA 的电子认证服务运营体系构成；
   (13) DFCA 的电子认证服务技术体系构成；
   (14) 灾难恢复和业务连续性管理；
   (15) 其他必要的培训。

5.3.3 工作轮换周期和顺序

对于可替换角色，DFCA 将根据业务的安排进行工作轮换。轮换的周期和顺序，视业务的具体情况而定。

工作岗位轮换遵循国家电子认证服务管理相关规范要求的职责分割的要求。

5.3.4 未授权行为的处罚

当 DFCA 的员工被怀疑，或者已进行了未授权的操作，例如，滥用权利或超出权限使用 DFCA 或进行越权操作，DFCA 得知后将立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。对情节严重的，依法追究相应责任。

5.3.5 独立合约人的要求

对不属于 DFCA 内部的工作人员，但从事 DFCA 有关业务的人员等独立签约者，DFCA 的统一要求如下：

1. 人员档案进行备案管理；
2. 签署保密协议；
3. 必须接受 DFCA 组织的相关知识与安全规范培训；
4. 由 DFCA 派专人监督和陪同从事相关在工作。

5.3.6 提供给员工的文档

为使得系统正常运行，必须提供给具有权限的相关人员各种文档，主要包括（但不限于）：

1. 认证系统相关软、硬件的操作手册，例如，认证系统操作手册、密码设备订户手册、目录服务器安装配置说明文件等；
2. 电子认证业务规则与相关的协议和规范；
3. 系统运行与维护相关的流程、管理办法，例如，机房设备管理办法；

电子认证服务相关的宣传资料；

5.4 审计日志程序

5.4.1 记录事件的类型

DFCA 记录与系统相关的事件，这些记录信息称为日志。对于这些日志，无论其载体是纸张还是电子文档的形式，必须包含事件发生的日期、事件的发生时间段、事件的内容和事件相关的实体等。DFCA 还可能记录其他与系统不直接相关的事件，例如：物理通道参观记录、人事变动等。

DFCA 持续、完整地记录关键操作与事件，包括但不限于：

1. 根证书密钥操作：包括密钥和生成、备份、存储、恢复、归档、销毁，以及密码设备的启用、停用、转移和销毁等；
2. 系统访问行为：包括所有对系统的访问企图，包括成功的和失败的登录、退出、权限使用行为等；
3. 系统操作与变更：包括对系统的各种关键查询、修改、删除等操作，系统组件的安装、升级、维修，人员，以及敏感信息的获取与取阅等；
4. 网络安全事件：包括防火墙、路由器、入侵检测安全设备记录的告警信息，以及针对被攻击事件识别与相应处理过程、结果等；
5. 证书生存周期关键过程：包括记录证书申请、审核、签发、更新、变更、撤销、冻结、恢复等操作，CRL 的签发与发布等，所有操作的通过或拒绝结果均应明确记录；
6. 机房门禁控制等物理环境事件，包括业务人员、安全运维人员、外部人员等在不同安全区域的进出记录等。

5.4.2 记录内容

每个事件记录应包含时间、类型、内容、操作人、作用对象及结果。对系统的关键操作应由操作人员进行电子签名。

5.4.3 保存期限

系统日志应至少保存至相关证书失效后五年，并实施严格的访问控制以防篡改或删除。

5.4.4 日志审计

5.4.4.1日志审计综述

日志审计内容，主要包括核实系统和操作人员的合规性包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

DFCA 至少每季度对系统日志进行一次审计，形成审计报告，并基于结果采取改进措施。

DFCA 的审计日志的保存期限不少于 5 年。

5.4.4.2审计日志的保护

DFCA 执行严格的管理，确保只有 DFCA 授权的人员才能对审查日志进行相应操作。日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、修改和删除等操作。

5.4.4.3审计日志备份程序

DFCA 保证所有的审查记录和审查总结都按照 DFCA 备份标准和程序进行备份。根据记录的性质和要求，按月进行备份，可采用在线和离线两种方式备份。

5.4.4.4审计日志收集系统

审计日志收集系统涉及：

1. 证书管理系统；
2. 密钥管理系统；
3. 证书注册管理系统；
4. 证书服务系统；

5. 证书在线业务门户；

6. 网站、数据库安全管理系统；

7. 其他需要审计的系统。

DFCA 使用系统审计工具对上述审计日志进行收集。

5.4.5 对导致事件实体的通告

DFCA 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，DFCA 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。

DFCA 有权决定是否对导致事件的实体进行通告。

5.4.6 脆弱性评估

DFCA 每年对系统进行脆弱性评估，以降低系统运行的风险。

5.5 记录归档

5.5.1 归档记录的类型

归档记录包括所有审计数据、证书申请信息、与证书申请相关的信息和证书信息等，主要包括：

1. 证书申请材料和订户意愿记录

2. 所有审计日志；

3. 密码设备全生存周期管理记录；

4. 密码设备的日常操作与使用记录

5. 根证书或密钥生存周期管理相关的全部记录，

6. 证书认证系统运行日志，

7. 已识别的安全事件及处置记录；

8. 证书认证系统关键操作日志，

9. 电子认证服务过程中其他操作记录。。

5.5.2 归档记录的保存期限

除了法律法规和管理部门提出的保存期限外，DFCA 对与证书相关的归档记录至少保存到证书有效期结束后 5 年。与法律政策的规定不一致时，选择两者中较长的期限予以保存。

此外，在不违反法律法规和管理部门的规定的前提下，DFCA 可以自主决定信息的存档期限，并不对此做出说明和解释。。

5.5.3 归档文件的保护

对电子归档记录采取技术手段保障其完整性，并存储在安全的物理与数字环境中，建立备份机制。存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能查询。DFCA 保护相关的档案内容，免遭恶劣环境的威胁，如温度、湿度和强磁力等的破坏。

DFCA 保存的申请信息、订户基本情况资料和身份鉴别资料，非经政府主管机构或司法机构经过合法途径予以申请，任何无关的第三方均无法获知。

DFCA 设立专门的档案管理机构统一管理归档记录，制定相关管理办法，明确管理职责、操作规范和安全要求。

5.5.4 归档文件的备份程序

所有存档的文件和数据库除了保存在 DFCA 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。DFCA 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。

5.5.5 记录时间戳要求

DFCA 暂不采用时间戳技术表明存档时间。

5.5.6 归档收集系统

认证系统的相关运营信息，由 DFCA 内部的工作人员或者具备完全控制措施的内部系统，依照人工和自动操作两部分进行产生的收集，并且由具备相关权限的人进行管理和分类。

5.5.7 获得和检验归档信息的程序

只有 DFCA 授权的可信人员能够访问归档记录。归档记录的一致性在归档时进行验证。归档期间，所有被访问的记录在归还时必须验证其一致性。

5.6 电子认证服务机构根证书密钥更替

5.6.1 密钥更替的情形

DFCA 密钥更替指 DFCA 认证机构证书到期时，需要更换密钥而采取的措施。

DFCA 密钥更替分为以下两类：

1. 紧急更类：发现密钥泄露或存在安全隐患，立即启动密钥更替程序；
2. 到期更替：宜在密钥到期前二年完成密钥更替。

5.6.2 密钥更替的流程

DFCA 密钥更替流程如下：

1. 密钥生成：在颁发或更换根证书时，在安全可靠的环境中生成新密钥对，具体见 6.2；
2. 申请新 CA 根证书：，DFCA 将向国家根 CA 机构申请新 CA 根证书；
3. 根证书发布：将新的 CA 公钥证书发布给证书订户和依赖方；
4. 旧密钥处理：在完成签名密钥更替后，按 GB/T 25056-2018 中 8.2.4.3 规定的

方式，销毁旧私钥及其备份，并保留相关操作记录。

5.7 损害和灾难恢复

5.7.1 业务连续性目标

DFCA 的业务连续性目标如下：

1. 灾难恢复的恢复时间目标（RTO）：2 小时
2. 恢复点目标（RPO）：2 小时

5.7.2 事故和损害处理程序

发生故障时，DFCA 将按照灾难恢复计划实施恢复。

5.7.3 恢复流程

5.7.3.1 证书库恢复流程

当 DFCA 的证书库出现损毁、泄露等情况时，DFCA 采取如下措施处理：

1. 立即向电子认证服务主管部门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，采取措施保证订户利益不受损失；
2. 使用备份数据恢复系统与系统数据库；
3. 根据证书申请记录，重新处理受影响的证书申请；
4. 同步目录服务器；
5. 通知受影响的订户，重新下载证书。

5.7.3.2 DFCA 私钥损害恢复流程

当 DFCA 的根私钥出现损毁、遗失、泄露、破解、被篡改、或者有被第三者窃用的疑虑时，DFCA 采取如下措施处理：

1. 立即向电子认证服务主管部门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，采取措施保证订户利益不受损失；
2. 立即撤销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。同时，立即生成新的密钥对，并自签发新的根证书；
3. 新的根证书签发以后，按照本 CPS 关于证书签发的规定，重新签发下级证书和订户证书；
4. 新的根证书签发以后，将立即通过 DFCA 的信息库、目录服务器、门户网站等方式进行发布。

订户的私钥出现损毁、遗失、泄露、破解、被篡改、或者有被第三者窃用的疑虑时，订户应按照本 CPS 的规定，首先申请撤销证书，然后按照规定重新申请新的证书。

5.7.3.3 其他关键资产恢复流程

DFCA 遭到攻击，发生 CA 物理设施、计算资源、网络环境、软件遭受毁坏，其他密钥数据或数据库被篡改等现象或因不可抗力造成灾难，DFCA 将按照灾难恢复计划实施恢复。

5.7.3.4 灾难后的业务连续性能力

针对 DFCA 的核心业务系统采用双机备份方式；对核心数据库，证书管理系统数据库采用磁盘阵列方式来确保证书系统的高可靠性和可用性。

发生自然或其它不可抗力性灾难后，DFCA 可采用备份恢复方式对运营进行恢复。具体的安全措施按照 DFCA 灾难恢复计划实施。

5.7.4 根私钥应急处理

DFCA 制定《CA 密钥应变处理实施细则》，建立根私钥泄露的应急流程，明确应急响应时间要求、责任人员、处置步骤和上报机制。

DFCA 每年进行一次应急演练。

5.7.5 事件报告

发生灾难并实施恢复计划的事件，DFCA 及时向有关主管部门报告。具体流程与要求见 5.9。

5.7.6 定期验证

DFCA 定期验证备份的设备、数据可用性，包括备份恢复测试和功能验证，每年至少进行一次灾难恢复演练。

5.8 电子认证服务机构终止

因技术性原因或商业原因等，DFCA 需要终止运营时，将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

1. 在暂停或者终止服务九十日前，就业务承接及其他有关事项向证书持有者以及其他所有相关实体进行通告。至少提前六十日向主管部门报告；
2. 确定具有资质的电子认证服务业务承接单位，签署承接协议，明确约定承接机构的工作范围与责任；
3. 保存所有的认证服务相关运营资料，包括（但不限于）证书、订户信息、系统文件、CPS、规范与协议等；
4. 向承接方移交密钥及相关关键数据，协调承接单位启动相关运营工作；
5. 停止证书状态服务并归档相关数据；
6. 停止其他电子认证相关服务并归档相关数据；
7. 停止密码设备并归档相关密钥数据；
8. 及时撤销或冻结业务管理员和业务操作员的操作权限；
9. 对所有存档文件记录进行整理和封存；
10. 对所有敏感文件和数据进行安全处理和封存；

11. 清除主机和密码硬件设备中的敏感数据；

12. 保存其他涉及 CA 运营的数据、密钥；

13. 机构发布终止服务通告。

当 DFCA 授权的证书服务机构因故终止服务时，DFCA 将按照与其签订的相关协议处理有关业务承接事宜与其他事项。因 RA 故终止服务时，DFCA 将按照与 RA 签订的相关协议处理有关业务承接事宜与其他事项。

5.9 重大事项报告

5.9.1 重大事项报告的情形

在 DFCA 开展电子认证服务过程中，若发生重大事件，需及时向公司管理屋、上级机构和主管部门进行报告。重大事件包括但不限于：

1. 证书认证系统迁移或改造，包括系统软件、网络、部署的重大改变。具体包括以下情形：

   (1) 机房迁移，或机房内服务区、管理区或核心区划设范围改变；

   (2) 数字证书认证系统软件升级或变更

   (3) 变更电子签名认证证书签发逻辑；

   (4) 新增远程证书注册子系统；

   (5) 新增、更改或者删除用于签发电子签名认证证书的证书链；

   (6) 其他对电子认证服务安全、用户资料安全有影响的改变。

2. 重大安全事故：包括电子认证服务系统遭受黑客攻击、病毒入侵、数据泄露等，导致系统无法正常运行或数据安全性受到严重威胁的情形：

   (1) 证书签发及验证服务连续停机时间超过 24 小时；

   (2) 发生根证书密钥等关键数据泄露；

   (3) 持续或较大范围未经授权的私钥访问记录或其他异常活动；

   (4) 系统日志持续或较大范围显示异常操作（如非授权时间或网络地址访问敏感功

能）。

3. 订户信息泄露事件：包括订户身份信息、证书申请资料等敏感数据被泄露等：

   (1) 个人信息泄露事件影响范围较广，造成一定的经济损失或客户投诉；

   (2) 数据丢失导致无法恢复证书状态信息。

4. 合规性事件：包括不符合相关法律法规、标准或监管要求的情形：

   (1) 涉及电子认证服务的司法判定；

   (2) 收到行政部门违规通知或处罚决定。

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

   (1) 涉及 2 名及以上管理层人员或 10%以上可信人员的离职；

   (2) 劳动纠纷参与人数超过员工总数 10%，且经法院或仲裁机构生效裁决确认由 CA 承担法律责任。

6. 其他事件：其他对电子认证服务运营产生巨大影响的事件。

5.9.2 重大事项报告的流程与时限

为保障重大事件及时响应、闭环处置，DFCA 对重大事项报告的时限规定如下：

1. 所有在岗运维、审核、值班及业务管理人员，在发现或接报疑似重大事件后，需第一时间完成事件初步甄别与确认，不得拖延、瞒报、漏报或谎报。确认属于重大事件范畴的，需在 15 分钟内完成内部紧急初报，通过口头、即时通讯等方式上报 DFCA 的安全管理负责人、业务运营负责人及应急管理部门，同步简要说明事件发生时间、初步现象、影响业务范围及现场处置初步动作，实现风险快速预警；

2. 在完成紧急初报后的 1 小时内，根据整合现场排查信息，形成正式书面初步报告，详细记录事件基本情况、初步排查原因、受影响的系统、证书用户范围、当前处置措施及风险预判，完成内部层级审批上报，同步更新事件处置动态；

3. 对于符合行业监管报备标准的重大事件，DFCA 严格遵照国家电子认证服务相关管理规定，在事件确认后的 24 小时内完成向行业监管部门的正式报备工作，如实提

交事件概况、处置进展、风险防控措施等相关材料，主动接受监管监督；

4. 在事件完全处置完毕、系统服务恢复正常、风险彻底清零后，在 24 小时内完成完整复盘报告的编制工作，全面梳理事件发生根源、完整处置流程、造成的影响与损失、存在的管理漏洞，同步制定对应的整改优化措施、长效防控方案及责任认定结果。

DongFang eTrusted Certification Authority Center of China 东方新诚信数字认证中心 .DFCA.

6 认证系统技术安全控制

6.1 技术安全管理制度要求

DFCA 已建立并实施履盖“密钥管理、数据管理、系统开发、网络防护、物理环境管理”等领域的技术安全管理制度，并定期接受安全策略委员会的评审，频率不低于每年一次。

6.2 密钥对的生成和安装

6.2.1 根证书密钥对的生成和安装

CA 系统的根密钥由国家密码管理部门认可的硬件密码机独立生成，密码机部署在屏蔽机房当中，操作人员只能在屏蔽机房中对根密钥进行操作。

根密钥的生成、备份、恢复、销席过程应实施 5 选 3 多人控制机制。

密钥操作需向安全策略委员会提交书面申请，并经安全策略委员会授权后方可实施。

所有操作需通过录音录像方式全程记录，保存期限不少于操作完成后十年。

6.2.2 订户密钥对的生成和交付

订户签名密钥对的生成，采用以下方式之一：

1. 由订户持有的、国家密码管理部门认可的密码模块生成和存储；

2. 经订户委托，由 DFCA 生成、保存，并提供技术措施确保订户对签名私钥的独占控制权。

订户的加密密钥对（包括加密公钥、加密私钥）由 DFCA 的密钥管理中心生成。加密私钥存储在订户的密码模块与密码管理中心的密钥数据库中。密钥数据库的密钥数据以加密方式存储。

DFCA 完整记录所有与订户签名私钥相关的操作日志，包括时间、方式、操作人员等信息，保存期限不少于证书失效后五年。

订户的签名密钥对由订户自己生成并保管。

加密密钥对由密钥管理中心产生，通过安全通道传到订户的密码模块。

6.2.3 公钥传送给证书签发机构

在公钥传递过程中，DFCA 采用国家密码管理局许可的通讯协议及密钥算法，保证传输中数据的安全。

6.2.4 电子认证服务机构公钥传送给依赖方

依赖方可以从 DFCA 的网站下载认证机构证书，从而得到 DFCA 的公钥。

6.2.5 密钥的长度

DFCA 支持 RSA 算法与 SM2 算法。RSA 非对称密钥对的模长是 1024 比特，SM2 非对称密钥对的长度是 256 比特。

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

6.2.6 公钥参数的生成和质量检查

公钥参数由国家密码管理局许可的密码设备产生。

公钥参数质量的检查同样通过国家密码管理局许可的密码设备进行。

6.2.7 密钥使用目的

CA 密钥：用于签发证书和 CRL。

订户密钥：订户的签名密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等，加密密钥可以用于信息加密和解密。签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

6.3 私钥保护和密码模块工程控制

6.3.1 CA 私钥保护和密码模块工程控制

6.3.1.1 CA 私钥的密码模块标准和控制

DFCA 的根密钥的生成、存储与保护，使用通过国家密码主管部门认可的密码产品，符合 GB/T 37092-2018 第 5 章的要求。

6.3.1.2 CA 私钥的多人控制

DFCA 的根私钥的生成、更新、注销、备份和恢复等操作采用多人控制机制，即采取 5 选 3 方式，将私钥的管理权限分散到 5 张密钥卡中，只有其中至少 3 人在场并许可的情况下，才能对私钥进行上述操作。

6.3.1.3 CA 私钥备份

根密钥备份数据由不同的密钥管理员分别保存在屏蔽机房的保险柜与银行保险箱中。

6.3.1.4 CA 私钥的激活方法

DFCA 的 CA 私钥存放于密码设备中，其激活数据保存于 IC 卡介质中，必须采用 5 选 3 的方式分别输入激活数据才能激活。激活私钥至少需要 3 名密钥管理员同时在场，使用智能 IC 卡登录加密机，启动密钥管理程序，进行激活私钥的操作。

6.3.1.5 解除私钥激活状态的方法

具有解除私钥激活状态权限的管理员使用含有自己身份的密码设备登录，启动密钥管理程序，进行解除私钥的操作，需要 3 名管理员同时在场。

6.3.1.6 CA 私钥的销毁方法

具有销毁密钥权限的管理员使用含有自己身份的密码设备登录，启动密钥管理程序，进行销毁密钥的操作，需要三名管理员同时在场；同时，所有用于激活私钥的 PIN 码、IC 卡、动态令牌等密码设备也必须被销毁或者收回。

6.3.1.7 密码模块的评估

DFCA 使用国家密码主管部门批准和许可的密码设备。根据 DFCA 对密码设备的性能、工作效率、供应厂商的资质等方面的评估，选择需要的密码模块。

6.3.2 订户私钥保护和密码模块工程控制

6.3.2.1 订户私钥的密码模块标准和控制

订户的签名私钥的生成、存储，使用通过国家密码主管部门认可的密码模块。签名私钥由订户持有，在 DFCA 与订户签署的服务协议中要求订户采取预防措施防止私钥及其激活数据的丢失、泄露、更改或未经授权的使用。

订户的加密密钥由密钥管理中心使用国家密码主管部门批准和许可的硬件密码设备生成，加密保存在数据库中。

订户在下载证书时，加密密钥对使用用户的签名公钥进行加密保护。以密文方式导入到订户的密码模块。

目前，DFCA 不提供订户签名私钥的委托保管服务。

6.3.2.2 订户私钥备份

订户的签名密钥 DFCA 不予备份。加密密钥由 DFCA 的密钥管理中心备份，备份数据以密文形式保存。

6.3.2.3 订户私钥的激活方法

订户私钥由订户输入 PIN 进行激活。订户可以通过 DFCA 提供的工具自行设置 PIN。

6.3.2.4 密码模块的评估

DFCA 使用国家密码主管部门批准和许可的密码设备。根据 DFCA 对密码设备的性能、工作效率、供应厂商的资质等方面的评估，选择需要的密码模块。

6.4 密钥对管理的其他方面

6.4.1 公钥归档

订户证书中的公钥包括签名公钥和加密公钥。公钥的归档，其操作过程、安全措施、保存期限以及保存策略和证书保持一致，归档要求参照本 CPS 中“5.5 记录归档”的相关规定

DFCA 每天对公钥证书进行归档。

6.4.2 证书操作期和密钥对使用期限

所有证书的有效期和其对应的密钥对的有效期都是一致的。无论是订户证书还是 CA 证书，证书到期后，签名私钥不可用于电子签名。

根证书密钥对的有效期为 20 年。

订户证书密钥对的最长有效期为 5 年。

6.5 激活数据

激活数据用于保护订私钥。

CA 私钥的激活数据，由 DFCA 的不同密钥管理员妥善保管。见 6.3.14。

订户私钥的激活数据，在证书存储介质（如：智能密码钥匙）出厂时设置了缺省的 PIN 值。DFCA 在证书制作时更改此 PIN 值并通过安全的方式告知订户，订户可以自行设置或更改。

6.6 计算机安全控制

应在 CPS 中明确建立并实施符合 GB/T 25056-2018 中 8.2 要求的计算机安全控制体系，包括但不限于：

a) 至少每半年检查一次系统升级补丁，记录系统升级审批及实施过程；

b) 对无官方补丁支持的系统，制定网络隔离、功能限制等加强防护措施和系统更替计划；

c) 对所有服务器和操作终端安装杀毒软件；

d) 病毒库更新间隔；

e) 病毒扫描时间间隔。

6.6.1 特别的计算机安全技术要求

为了保证系统的正常运行，对所需要的计算机设备进行正确的选型、验收，制定操作规范。DFCA 遵循 GB/T 25056-2018 中 8.2 要求，建立并实施对应的计算机安全控制体系。

1. 至少每半年检查一次系统升级补丁，记录系统升级审批及实施过程；
2. 对无官方补丁支持的系统，制定网络隔离、功能限制等加强防护措施和系统更替计划；
3. 对所有服务器和操作终端安装杀毒软件；
4. 病毒库更新间隔为一个月；
5. 病毒全盘扫描时间间隔为一周。

6.6.2 计算机安全评估

DFCA 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。同时，DFCA 已通过国家密码管理局组织的安全性审查。

6.7 生存周期安全控制

DFCA 建立并实施符合 GB/T 25056-2018 中第 10、11、12 章要求的生存周期安全控制体系。

6.7.1 系统开发控制

系统开发采用先进的安全控制理念，同时应兼顾开发环境的安全、开发人员的安全、产品维护期的配置管理安全。系统设计和开发运用软件工程的方法，做到系统的模块化和层次化，系统的容错设计采用多路并发容错方式，确保系统在出错的时候尽可能不停止服务。

6.7.2 安全管理控制

DFCA 的信息安全管理，严格遵循国家密码管理局等主管部门的有关运行规范和 DFCA 的安全管理策略进行操作。

DFCA 的使用具有严格的控制措施，所有和系统都经过严格的测试验证后才进行使用。任何修改和升级均记录在案并进行版本控制、功能测试和记录。DFCA 还对认证系统进行定期和不定期的检查与测试。

DFCA 采取严格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。

6.7.3 生命期的安全控制

整个系统从设计到实现，系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计，使用的算法和密码设备均通过了国家密码管理局的鉴定与安全性审查，使用基于标准的强化安全通信协议以确保通信数据的安全；在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施，整个系统安全可靠。

6.8 网络安全控制

DFCA 建立并实施符合 GB/T 25056-2018 中 5.3.8 要求的网络安全控制体系，包括但不限于：

1. 网络结构满足 GB/T 25056-2018 附录和 A 中规定形式的一种；
2. 对所有 Web 服务配置防火墙、Web 应用防火墙、入侵检测系统和内容过滤等网络安全防护措施；
3. 建立并维护网络拓扑图，包含所有网络设备、连接关系和安全边界，定期更新，与机房实际情况保持一致；
4. 网络访问控制：
   (1) 建立针对证书签发子系统及数据库的访问自名单机制，仅授权证书注册子系统的必要功能模块及必要的管理设备进行访问；
   (2) 建立针对证书注册子系统和数据库的访问白名单机制。
5. 网络监控：
   (1) 每周对系统日志进行分析；
   (2) 分析内容包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

6.9 时间戳

DFCA 暂未采用时间戳技术。

7 证书、证书撤销列表和在线证书状态协议

7.1 证书

DFCA 签发的电子签名认证证书符合 GB/T 20518 的要求，包括的主要信息项说明如下：

1. 数字证书格式版本号：V3
2. 签名算法标识：SM3WithSM2（1.2.156.10197.1.501）
3. 颁发者名称：CN = DongFang eTrust CA V2, O = DongFang eTrust Digital Certificate Center, L = Changsha, S = Hunan, C = CN
4. 订户名称：（由订户在申请时定义）
5. 证书序列号：证书签发时生成，10 位以上大整形数。证书序列号是证书的唯一标识，所有由 DFCA 签发的电子签名证书，其序列号是唯一的；
6. 证书有效期：（由订户在申请时指定，最大不超过 5 年）
7. CA 的电子签名：由 DFCA 在签发证书时生成
8. 证书策略标识：（根据证书类型，由 DFCA 在签发证书时指定，具体取值见 1.5.2.1 的表 1-1）
9. 密钥用途。主要包括：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、只签名等；
10. 基本限制。用于鉴别证书持有者身份；
11. CRL 发布点。东方新诚信认证系统定义的 CRL 发布点；

7.2 证书撤销列表

DFCA 签发的证书撤销列表（CRL），符合 GB/T 20518-2018 中 5.3 的要求。主要信息项说明如下：

1. 版本号： V2
2. 颁发者名称：CN = DongFang eTrust CA V2, O = DongFang eTrust Digital Certificate Center, L = Changsha, S = Hunan, C = CN
3. 授权密钥标识符：DFCA 的运营 CA 根密钥标识符；
4. CRL 条目扩展项：不使用 CRL 条目扩展项。

7.3 在线证书状态协议

DFCA 提供的在线证书状态服务，符合 GB/T 19713-2025 中第 7 章的要求。

在线证书状态服务使用的是 OCSP 版本 1（OCSP v1）

8 认证机构审计及相关评估

8.1 审计评估制度

8.1.1 审计评估的类型与方式

审计是为了检查、确认 DFCA 是否按照本 CPS 及其业务规范、管理制度和安全策略开展业务，发现存在的可能风险。

DFCA 制定了《安全审计管理办法》等审计评估制度，明确了审计评估的相关要求。

审计评估的类型，认证业务审计和全面符合性评估：

1. 认证业务审计：对 DFCA 日常的“电子认证业务活动”做合规性、真实性、安全性的检查与审计。涵盖“证书申请、业务告知、意愿确认、身份核验、协议签署、证书签发、证书存储、证书分发、证书撤销、资料归档、证书/CRL 发布全生命周期的业务流程、人员操作、系统日志、证据留存、权限控制、密钥管理、事件处置等方面的内容；
2. 全面符合性评估：对 DFCA 整体“是否符合所有标准与规范”进行全面、系统、结论性的评估。涵盖 DFCA 的”技术体系、安全控制、密码算法、协议实现、系统配置、管理制度、人员能力、灾备与连续性、OCSP/CRL 服务、证书格式、签名算法（如 SM3WithSM2）”等方面的内容。

审计评估方式分为内部审计和外部审计。

1. 内部审计是由 DFCA 的安全策略委员会组织内部人员进行的审计，审计的结果用于 DFCA 改进、完善电子认证业务；
2. 外部审计由 DFCA 委托第三方专业审计机构来承担。

根据《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》、《电子政务电子认证服务管理办法》的规定，接受管理部门的评估和检查。

8.1.2 审计评估的频率

根据审计类型、审计方式，审计评估的频率要求如下：

1. 全面符合性评估：DFCA 每年至少组织一次全面符合性评估，采用外部外部审计方式；
2. 认证业务审计：DFCA 每半年组织一次认证业务审计，采用内部审计方式；
3. 若发生重大业务事件，经安全策略委员会批准，组织开展认证业务审计。根据实际情况，可采用内部审计方式或外部审计方式。

8.1.3 外部审计机构的要求

执行外部审计的审计机构，需满足如下要求：

1. 为中华人民共和国国内注册的独立法人，与 DFCA 无股权/管理关联，能独立承担法律责任；
2. 具有商用密码检测机构资质（国家密码主管部门认定），资质范围含商用密码应用评估、密钥安全、证书系统检测等；
3. 具有电子认证服务相关审计资质；
4. 上述审计资质在审计周期内持续有效；
5. 近 3 年无重大违法、处罚或失信记录，无被监管撤销资质情形；
6. 未向 DFCA 提供咨询、运维、技术开发、密钥托管等服务。

8.1.4 外部审计机构的审计人员的专业要求

执行审计的外部审计机构的审计人员，需具有如下资质要求：

1. 项目负责人，具备 CISA/CISSP/注册信息安全专业人员（CISP）之一，且有大于 5 年（含 5 年）的电子认证业务/公开密钥体制/密码安全审计经验；
2. 核心审计员，需满足以下要求：
   (1) 至少 2 人，均需具备密码学/网络安全/电子认证背景，持有国家密码主管部门认定的检测人员证书；
   (2) 至少 1 人熟悉 SM2/SM3/SM4、国密算法合规、《电子认证服务管理办法》、《电子认证业务规则规范》、GB/T 相关、GM/T 系列等标准规范。

(3) 能独立开展“密钥审计、根/中间证书生命周期审计、CRL/OCSP 系统审计、日志溯源、渗透测试、漏洞评估”等审计工作。

(4) 至少 1 人，具有近 3 年至少 3 家同类第三方 CA 全审计案例。

8.2 认证业务审计

认证业务审计对 DFCA 日常的“电子认证业务活动”做合规性、真实性、安全性的检查与审计，具体要求如下：

1. 认证业务审计的审计周期，具体要求如下：
   (1) 一般情况下，每半年开展 1 次；
   (2) 若遭遇高风险事件或重大事件，经安全策略委员会批准后，可随时启动认证业务审计。
2. 审计内容包括但不限于“证书申请、续期、密钥变更、更新、撤销、冻结等业务中订户告知、身份查验、意愿记录、协议签署、资料保存”等业务操作的合规性；
3. 对于认证业务审计的审计方式，规定如下：
   (1) 每 2 年应至少组织 1 次全面审计；
   (2) 采用抽样审计方式，审计抽样率不低于 10%。
4. 对于审计发现的问题，通知相关部门和人员及时整改。相关部门在 5 个工作日内需提交整改工作，提出相关问题的整改措施；
5. 安全策略委员会指定专人跟踪整改落实情况，最迟在次月的安全策略委员会会议对整改情况进行全面总结。

8.3 全面符合性评估

对 DFCA 整体“是否符合所有标准与规范”进行全面、系统、结论性的评估，具体要求根号如下：

1. 每年至少组织一次全面符合性评估；
2. 评估内容包括但不限于：年度电子认证服务开展情况、电子认证服务许可条件符合性情况以及认证规则和证书策略符合性情况等；
3. 对于全面符合性评估的审计方式，规定如下：
   (1) 每 2 年应至少组织 1 次全面审计；

(2) 采用抽样审计方式，审计抽样率不低于 10%。

4. 对于审计发现的问题，通知相关部门和人员及时整改。相关部门在 5 个工作日内需提交整改工作，提出相关问题的整改措施；
5. 安全策略委员会指定专人跟踪整改落实情况，最迟在次月的安全策略委员会会议对整改情况进行全面总结；
6. 在每年 1 月底前将上一年度符合性评估报告报送主管部门。

9 法律责任和其他业务条款

9.1 费用

DFCA 开展服务成本核算，并据此制定电子认证服务价格策略。

电子认证服务收费标准在 DFCA 的官网上予以公示，具体收费内容与标准包括但不限于：

1. 各类证书业务费用：包括“颁发、更新、续期、变更、撤销、密钥恢复”等业务的费用；
2. 各类证书载体的费用；
3. 状态信息访问费用；
4. 电子签名的费用；
5. 签名验证的费用；
6. 签名验证报告的费用；
7. 其他服务的费用。

有关费用的退款方式，亦在 DFCA 的官网上予以公示。

9.2 财务责任

9.2.1 保险范围

出现下列情形并经公司确认后，证书订户、依赖方等实体可以申请赔偿（法定或约定免责除外）。

1. DFCA 在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发，并导致订户或依赖方遭受损失的；
2. DFCA 将证书错误的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；
3. 由于 DFCA 的原因导致证书私钥被破译、窃取，导致订户或者依赖方遭受损失的；

4. DFCA 未能及时撤销证书，导致订户或者依赖方遭受损失的。

9.2.2 资金保障与管理

DFCA 设立了专项备用资金，以保证其具有维持其运作和履行其责任的财务能力，资金保障额度不低于上一年度营业收入 1.5%。

资金来源于上一年度营业收入，并由财务部门设立专门账户进行管理。

9.3 业务信息保密

保密的业务信息包括但不限于以下方面：

1. 在双方披露时标明为保密（或有类似标记）的；
2. 在保密情况下由双方披露的或知悉的；
3. 双方根据合理的商业判断应理解为保密数据和信息的；
4. 以其他书面或有形形式确认为保密信息的；
5. 从上述信息中衍生出的信息。

对于 DFCA 来说，保密信息包括但不限于以下方面：

1. 最终订户的私人签名密钥都是保密的；
2. 保存在审计记录中的信息；
3. 年度审计结果也同样视为保密；
4. 除非有法律要求，由 DFCA 掌握的，除作为证书、CRL、认证策略被清楚发布之外的个人和单位的信息需要保密。

DFCA 不保存任何证书应用系统的交易信息。

除非法律明文规定，DFCA 没有义务公布或透露订户数字证书以外的信息。

9.3.1 不属于保密的信息

与证书有关的申请流程、申请需要的手续、申请操作指南等信息是公开的。DFCA 在处

理申请业务时可以利用这些信息，包括发布上述信息给第三方。

订户数字证书及注销信息不属于保密信息，通过 DFCA 目录服务等方式向外公布。

9.3.2 保护保密信息的责任

DFCA 或其注册机构、订户、依赖方等各参与方，均有按照本 CPS 规定，承担保护保密信息的责任。不将保密信息（也不会促使或允许他人将保密信息）用于协议项下活动目的之外的其他用途，包括但不限于：将此保密信息的全部或部分进行仿造、反向工程、反汇编、逆向推导；在披露当时，如果已明确表示保密信息不得复印、复制或储存于任何数据存储或检索系统，接受方不得复印、复制或储保密信息。

当 DFCA 在任何法律、法规或规章的要求下，或在法院的要求下必须提供本 CPS 中具有保密性质的信息时，DFCA 应按照要求，向执法部门公布相关的保密信息，DFCA 无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

当保密信息的所有者出于某种原因，要求 DFCA 公开或披露他所拥有的保密信息时，应书面授权以表示其自身的公开或者披露意愿，DFCA 应满足其要求。如该披露行为涉及任何其他方的赔偿义务和所造成的损失，应由保密信息的所有者承担，DFCA 不予承担。

9.4 个人隐私保护

9.4.1 隐私保密方案

DFCA 尊重所有用户及其隐私，个人隐私信息保密方案遵守现行法律和政策规定。

DFCA 遵循 GB/T 35273 的规定，制定个人隐私保护方案。

用户选择使用 DFCA 的服务，就表示已经同意接受 DFCA 有关隐私保护的声明。

9.4.2 作为隐私处理的信息

证书申请人提供的不构成数字证书内容的资料被视为隐私信息。

9.4.3 不被视为隐私的信息

证书申请人提供的用来构成数字证书内容的资料不认为是隐私信息。

数字证书是公开的，通过 DFCA 目录服务等方式向外公布。

9.4.4 保护隐私的责任

接收到隐私信息的参与者有责任保护隐私信息不被泄漏、使用或发布给第三方。

9.4.5 使用隐私信息的告知与同意

使用隐私信息，须获得本人同意。

9.4.6 依法律或行政程序的信息披露

当 DFCA 在任何法律、法规或规章的要求下，或在法院的要求下必须提供证书申请人的特定资料或隐私信息时，DFCA 按照法律、法规或规章的要求或法院的要求，向执法部门公布相关信息，DFCA 无须承担任何责任。这种提供不能被视为违反了隐私保护的责任和义务。

9.4.7 其他信息披露情形

其他信息的披露遵循国家的相关规定处理。

9.5 知识产权

除非额外声明，DFCA 享有并保留对证书以及 DFCA 提供的全部软件的一切知识产权，包括所有权、名称权和利益分享权等。DFCA 有权决定关联机构采用的软件系统，选择采取的形式、方法、时间、过程和模型，以保证系统的兼容和互通。

按本 CPS 的规定，所有由 DFCA 签发的证书和提供的软件中使用、体现和相关的一切版权、商标和其他知识产权均属于 DFCA 所有，这些知识产权包括所有相关纸质和电子文档。RA 等相关实体应征得 DFCA 的授权后才能使用相关文档，并有责任和义务提出修改意

见。

9.6 陈述和担保

9.6.1 电子认证服务机构的陈述与担保

DFCA 在提供电子认证服务活动过程中的承诺如下：

1. DFCA 遵守《中华人民共和国电子签名法》及相关法律的规定，接受信息产业部的领导，对签发的数字证书承担相应的法律责任；
2. DFCA 保证使用的系统及密码符合国家政策与标准，保证自身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定；
3. 除非已通过 DFCA 证书库发出了 DFCA 的私钥被破坏或被盗的通知，DFCA 保证其私钥是安全的；
4. DFCA 签发给订户的证书符合 DFCA 的 CPS 的所有实质性要求；
5. DFCA 将向证书订户通报任何已知的、将在本质上影响订户的证书的有效性和可靠性事件；
6. DFCA 将及时注销证书；
7. 证书公开发布后，DFCA 向证书依赖方证明，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。

9.6.2 RA 的陈述与担保

DFCA 的 RA 在参与电子认证服务过程中的承诺如下：

1. 提供给证书订户的注册过程完全符合 DFCA 的 CPS 的所有实质性要求；
2. 在 DFCA 生成证书时，不会因为 RA 的失误而导致证书中的信息与证书申请人的信息不一致；
3. RA 将按 CPS 的规定，及时向 DFCA 提交证书申请、注销、更新等服务请求。

9.6.3 订户的陈述与担保

订户一旦接受 DFCA 签发的证书，就被视为向 DFCA、RA 及依赖方作出以下承诺：

1. 订户需熟悉本 CPS 的条款和与其证书相关的证书政策，还需遵守证书持有人证书使用方面的有关限制；
2. 订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，可供 DFCA 或其 RA 检查和核实；
3. 订户应当妥善保管私钥，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的发生；
4. 私钥为订户本身访问和使用，订户对使用私钥的行为负责；
5. 一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄密以及其他情况，订户应立刻通知 DFCA 或其 RA，申请采取注销等处理措施；
6. 订户已知其证书被冒用、破解或被他人非法使用时，应及时通知 DFCA 注销其证书。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉本 CPS 的条款以及和订户数字证书相关的证书政策，并确保本身的证书用于申请时预定的目的。

依赖方在信赖订户的数字证书前，必须采取合理步骤，查证订户数字证书及数字签名的有效性。

所有依赖方必须承认，他们对证书的信赖行为就表明他们承认了解本 CPS 的有关条款。

9.6.5 其他参与者的陈述与担保

其他参与者的陈述与担保同“9.6.4 依赖方的陈述与担保”。

9.7 担保免责

DFCA 在下列情况下免于承担责任：

1. 不对由于客观意外或其他不可抗力事件造成的操作失败或延迟承担任何赔偿责任。这些事件包括但不限于劳动纠纷、交易一方故意或无意的行为、罢工、暴动、骚动、战争、火灾、爆炸、地震、水灾或其他大灾难等；
2. 如果由于非东方新诚 CA 的原因而造成的设备故障、线路中断，导致签发数字证书错误、延误、中断或无法签发，DFCA 不负任何赔偿责任；
3. 本 CPS 的内容，没有任何信息可以暗示或解释成，DFCA 必须承担其他的义务或 DFCA 必须对其行为作出其他承诺。包括不承担其他任何形式的任何保证和义务，任何对特殊目的适用性的保证；
4. 如果申请者故意或无意地提供不完整、不可靠或已过期的，包括但不限于伪造、篡改、虚假的信息，而其又根据正常的流程提供了必须的审核文件，由此得到了 DFCA 签发的数字证书。由此引起的法律问题、经济纠纷应由申请人全部承担，DFCA 不承担与该证书内容相关的法律和经济责任，但可以根据受害者的请求提供协查和举证帮助；
5. DFCA 不承担任何其他未经授权的人或组织以 DFCA 名义编撰发表或散布不可信赖的信息所引起的法律责任；
6. 对于由于证书、签名或根据本 CPS 而提供或设计的任何其他交易或服务的使用、签发、授权、执行或拒绝执行而导致的或与之有关的任何间接性的、特别性的、附带性的、或结果性的损失，或任何利益损失、数据丢失，或其他间接性的、结果性的或惩罚性损失，无论是否可以合理预见，DFCA 将不会对此负责，即使 DFCA 曾经警告过这种损害的可能性；
7. DFCA 对签发的各类证书的适用范围有明确的规定，若证书订户将其证书用于其他不被允许的用途，DFCA 不承担任何责任，无论这种使用是滞造成损失；
8. DFCA 在法律许可的法律内，根据法律、政策等以及受害者的要求，如实提供不可抵赖的电子签名依据，但并不对此承担法律或政策规定之外的责任。

9.8 偿付责任规则

DFCA 制定偿付责任规则，内容包括但不限于：

1. 财务赔偿范围，涵盖 CA 在履行其服务职责时可能面临的各种风险，包括但不限于技术故障、人为错误、安全漏洞等，详见”9.9.1 赔偿范围”；
2. 明确界定不同情形下的赔付计算方式，详见“9.9.2 赔偿限额”；
3. DFCA 设立赔付监督机制，对赔偿的处理情况进行监督。

9.9 赔偿

应在 CPS 中明确赔偿的申请、审核、审批和支付疲程，明确各环节时限。

9.9.1 赔偿范围

在认证活动中产生的赔偿，都以本 CPS 的规定为处理依据，法律法规另有要求的除外。

1. DFCA 的赔偿责任

(1) 在签发证书时，如果未按照本 CPS 的规定进行处理，或者违反法律法规的要求而造成的证书订户损失的，DFCA 应承担赔偿责任；

(2) 因为操作人员恶意、故意或疏忽，未按照本 CPS 的规定办理证书的签发、注销等请求，布造成证书订户损失的，DFCA 应赔偿订户的损失；

(3) 因 DFCA 的根密钥出现问题，造成订户证书出现问题，DFCA 应赔偿相关损失；

(4) 证书订户或其他有权提出注销证书的人提出注销请求后，到 DFCA 将该证书注销信息予以发布的期间，如果该证书被用以进行非法交易，或进行交易时产生纠纷的，如果 DFCA 按照本 CPS 的规范进行了有关操作，DFCA 不承担任何损害赔偿责任；

(5) 证书订户赔偿的追溯有效期限，按照法律法规的要求进行操作。

2. RA 的赔偿责任

(1) RA 及其操作人员没有妥善保管订户的注册和身份验证的相关隐私信息，而造成订户信息泄漏、被冒用、自发或者任意使用导致产生损失的，RA 应承担损害赔偿责

任；

(2) 如果因为操作人员故意、恶意或者疏忽，没有按照本 CPS 的规定办理证书服务注册，或者违反法律法规而造成订户损失的，RA 应赔偿订户的直接损失，以及其他随之产生的附带损失和相关补偿；

(3) 因为 RA 的原因造成系统或软件错误，未能在本 CPS 规定的时间内，将订户的证书申请、注销、更新等请求信息发给 DFCA，而导致订户或依赖方损失的，RA 应承担所有的损害赔偿责任；

(4) 该类赔偿的追溯有效期限，按照有关法律法规的要求进行操作。

3. 订户的赔偿责任

(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，导致造成 DFCA 及其授权的证书服务机构或者第三方遭受损害的，订户应赔偿一切损害责任；

(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 DFCA 及其授权的证书服务机构，以及不当交付他人使用造成 DFCA 及其授权的证书服务机构、第三方遭受损害的，订户应承担一切损害赔偿责任；

(3) 订户使用证书或者依赖方信任证书的行为，有违反本 CPS 及相关操作规范，或者将证书用于非本 CPS 规定的业务范围的，订户或者依赖方应自行承担一切损害赔偿责任；

(4) 订户使用或信赖证书时，未能按照本 CPS 等规范进行合理审核，导致 DFCA 及其授权的证书服务机构或者第三方遭受损害的，应由该订户承担一切损害赔偿责任；

(5) 证书订户或者其他有权提出注销证书的实体提出注销请求后，到 DFCA 将该证书注销信息予以发布期间，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 DFCA 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；

(6) DFCA 与之签署的协议另有赔偿规定的，参照其规定。

9.9.2 赔偿限额

DFCA 及其授权的 RA，对所有当事人（包括但不限于订户、申请者、接受者或信赖方）

的合计赔偿责任，不可能超过发下所述对这些证书的封顶赔偿金额：

对于有关一张特定证书的所有签名和交易处理的总计，DFCA 及其授权的证书服务机构对于任何人（或者其他实体）有关该特定证书的合计赔偿责任应该限制在一个不超出下述数额的范围内（单位：人民币元）

1. 个人类证书，不超过 2,000 元

2. 机构类证书，不超过 50,000 元

本条款限制用于一定形式的损害，包括但不限于任何人或实体（包括但不限于订户、证书申请者、接收方或者信赖方）由于信任或者使用 DFCA 签发、管理、使用或注销的证书或已过期证书而导致的直接的、补偿性的、间接的、特别的、结果的、惩戒性的或意外的损害。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的赔偿均有限额而不考虑签名、交易处理或其他有关的索赔数量。当超过赔偿限额时，除非得到依法判决或仲裁，可用的赔偿限额将首先分配给最早得到索赔解决的一方。DFCA 没有责任为每张证书支付高出赔偿限额总和的赔偿，而不管高出赔偿限额总和在索赔提出之间是如何分配的。

9.9.3 赔偿处理时限

订户自知道或应当知道损害事实之日起 1 年内提出书面赔偿申请。逾期视为自动放弃赔偿申请权利，DFCA 可拒绝受理。

9.10 有效期和终止

9.10.1 有效期限

本 CPS 自发布之日起正式生效。

本 CPS 中将详细注明版本号及发布日期。

9.10.2 终止

当新版本的本 CPS 正式发布生效时，旧版本的本 CPS 自动终止。

9.10.3 效力的终止与保留

本 CPS 的某些条款在终止后继续有效，如知识产权承认和保密条款。另外，各参与方应返还保密信息到其拥有者。

9.11 对参与者的个别通告与沟通

除非法律法规或者协议有特别的规定，DFCA 将以合理的方式与相关各方进行沟通。认证活动的某一参与方与另一参与方进行通信时必须使用安全通道，以使其通信过程在法律上有效。

9.12 修订和发布

9.12.1 修订程序

当本 CPS 不适用时，由 DFCA 的安全策略委员会组织 CPS 编写小组进行修订。

安全策略委员会指定 CPS 编写小组负责起草 CPS 形成讨论稿，并征求公司领导和各部门意见，达成一致意见后提交策略管理委员会审阅；CPS 编写小组依据策略管理委员会评审意见完成 CPS 修改、确定 CPS 版本号，并形成定稿，报安全策略委员会主任审批；安全策略委员会主任审批同意后，方可对外发布。

公司行政部门负责自发布之日起 30 天内向主管机构备案。

9.12.2 通知机制和期限

本 CPS 在 DFCA 的网站上发布。

版本更新时，最新版本的本 CPS 在 DFCA 的网站发布，对具体个人不做另行通知。

9.12.3 必须修改业务规则的情形

当管辖法律、适用标准及操作规范等有重大改变时，必须修改本 CPS。

9.13 争议处理与举证

应在 CPS 中明确：

a) 与 CP/CPS、电子认证服务相关的争议解决机制，包括争议的受理范围、处理流程、协商时限、调解规则，以及诉讼、仲裁等法定争议解决方式的管辖规则与适用条件；

b) 举证制度和能力体系覆盖证书全生存周期，包括但不限于：

1) 证书签发环节，身份验证记录、材料审查记录、告知记录、意愿确认记录等；

2) 签名环节，签名请求验证、签名操作日志、时间碳记录等；

3) 验证签名环节，验证请求记录、验证结果记录、异常情况处理记录等；

4) 提供举证材料的时间承诺。

9.13.1 总体说明

本节明确 DFCA 关于电子认证服务全流程争议解决机制、举证管理制度、全生命周期证据留存规范及举证服务时限承诺，适用于 DFCA 与订户、依赖方及相关第三方因 CP/CPS 执行、证书签发、证书使用、签名验证、证书撤销、服务履约等产生的各类争议处理与举证溯源工作。本机制遵循合法合规、公平公正、及时响应、全程可追溯的原则，保障各方合法权益。

9.13.2 争议解决机制

9.13.2.1 争议受理范围

受理范围包含但不限于：CP/CPS 规则执行争议、证书身份核验与签发争议、电子签名有效性争议、证书状态（有效/撤销/冻结/过期）争议、CRL/OCSP 查询服务争议、认证服务履约争议、举证溯源争议、赔偿责任争议、服务投诉与合规异议等所有与 DFCA 电子认证服务相关的民事与合规争议。

9.13.2.2 争议处理流程与协商时限

1. 争议发起：争议方需以书面形式（含加盖公章纸质文件、合规加密邮件、官方申诉系统工单）向 DFCA 争议处理部门提交争议申请，明确争议事项、发生时间、相关证书信息、诉求及佐证材料。
2. 受理回执：DFCA 在收到争议申请后，3 个工作日内完成材料初审，告知申请人是否受理、需补充的材料清单。
3. 内部协商核查：对受理的争议事项，DFCA 启动全流程溯源核查，调取证书全生命周期日志、核验记录、操作留存证据，15 个工作日内完成核查并出具书面协商处理意见；复杂疑难争议可延期，最长不超过 30 个工作日，并提前告知申请人延期原因。
4. 协商闭环：双方达成一致的，签署争议处理确认文件，完成整改、赔付、解释等闭环处置；协商未达成一致的，终止协商流程，告知申请人后续调解、仲裁、诉讼渠道。

9.13.2.3 调解规则

争议双方协商无法达成一致的，可自愿向属地电子认证服务行业主管部门、市场监管部门、密码管理部门或合法第三方调解机构申请行政调解、行业调解。DFCA 严格配合调解流程，按要求提交完整合规的认证服务证据材料，遵从合法有效的调解结果。

9.13.2.4 仲裁与诉讼管辖规则

1. 仲裁：争议双方可事前或事后约定合法有效的仲裁机构，按照对应仲裁规则开展仲裁程序，DFCA 全程配合举证与核查。
2. 诉讼：无仲裁约定的，任意一方可依法向 DFCA 机构住所地有管辖权的人民法院提起民事诉讼，适用中华人民共和国现行有效法律、法规及司法解释。
3. 适用条件：所有争议解决方式均优先遵循《中华人民共和国电子签名法》《中华人民共和国民法典》《商用密码管理条例》《电子认证服务管理办法》及本 CPS 规

范执行。

9.13.3 全生命周期举证制度与能力体系

9.13.3.1 举证制度与能力体系概述

DFCA 建立覆盖证书签发、电子签名、签名验证、证书注销/撤销、服务运维全生命周期的举证留存体系，实现全程留痕、不可篡改、可溯源、可举证，所有记录留存满足司法采信、监管核查、争议溯源要求。

9.13.3.2 证书签发环节举证留存内容

完整留存证书申请与签发全流程原始记录，包含但不限于：申请者身份信息核验记录、主体资质材料审查记录、人工审核操作日志、线上系统审核留痕、服务告知记录、用户证书申领意愿确认记录、证书申请工单、审批流转记录、密钥生成与绑定记录、证书签发时间戳、签发结果存档记录、驳回/通过原因记录等。所有记录真实完整、时序可追溯，杜绝篡改、删除、替换。

9.13.3.3 电子签名环节举证留存内容

针对电子签名操作全程留痕举证，包含但不限于：签名请求合法性验证记录、签名用户身份核验记录、签名操作行为日志、操作终端信息、网络访问日志、可信时间戳固化记录、签名算法调用记录、签名值生成留存记录、签名成功/失败结果记录、异常签名拦截与处置记录等，确保每一次电子签名行为可独立溯源、可司法举证。

9.13.3.4 签名验证环节举证留存内容

完整留存所有签名验证服务操作记录，包含但不限于：验证请求接收记录、验证主体与证书信息匹配记录、签名有效性校验日志、证书状态核验（有效/撤销/过期）记录、CRL/OCSP校验结果记录、验证时间戳、验证最终结果记录、异常验证行为、非法签名、过期证书签名、篡改文件验证等异常情况的处置日志与复盘记录。

9.13.3.5 其他配套举证留存内容

除上述核心环节外，同步留存证书续费、冻结、解冻、注销、撤销、密钥更新、设备变更、权限调整、应急处置、安全审计等全流程记录，构建完整的证据链，满足各类争议与核查举证需求。

9.13.4 举证服务时间承诺

1. 日常争议举证：收到合法有效的书面举证申请及完备材料后，DFCA5 个工作日内完成证据检索、核验、整理，出具合规、可采信的举证材料；复杂跨周期举证事项，最长不超过 10 个工作日并告知进度。
2. 司法/监管紧急举证：收到法院、仲裁机构、密码管理部门、行业主管部门的正式协助调查、举证函件后，3 个工作日内响应并提交合规证据材料。
3. 证据留存时限：所有认证业务、签名、验证、运维、审计相关日志与证据材料，自对应证书注销、过期、终止服务之日起留存不少于 5 年，满足司法追溯、监管抽查、争议复盘的长期举证要求。
4. 证据有效性承诺：DFCA 留存的所有举证记录均为系统原生日志、不可篡改固化记录、可信时间戳存证数据，具备真实性、完整性、连续性，可作为争议调解、仲裁、诉讼的有效证据。

9.13.5 举证责任与免责说明

1. 因 DFCA 系统故障、操作违规、流程疏漏导致证据缺失、记录异常的，DFCA 依法承担对应责任；
2. 因申请人/依赖方自身操作失误、密钥保管不当、私自篡改数据、未及时留存本地凭证导致的争议，由责任方自行承担责任；
3. DFCA 仅对自身认证服务流程内的原始记录承担举证责任，不对第三方终端、第三方系统、用户本地数据承担举证义务。

9.14 管辖法律

本 CPS 在各方面服从中国法律和法规的管制和解释，包括但不限于《中华人民共和国电子签名法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《商用密码管理条例》《电子认证服务管理办法》《电子认证服务密码管理办法》等。

9.15 与适用法律的符合性

无论在任何情况下，本 CPS 的执行、解释、翻译和有效性均适用中华人民共和国的法律。

9.16 一般条款

9.16.1 完整协议

本 CPS 将替代先前的、与主题相关的书面或口头解释。

9.16.2 转让

DFCA、RA、订户及依赖方之间的责任、义务不能通过任何形式转让给其他方。

9.16.3 分割性

当法庭或其他仲裁机构判定协议中的某一条款由于某种原因无效或不具执行力时，不会出现因为某一条款的无效导致整个协议无效。

9.16.4 强制执行

免除一方对合同某一项的违反应该承担的责任，不意味着继续免除或未来免除这一方对合同其他项的违反应该承担的责任。

9.16.5 不可抗力

不可抗力是指不能预见、不能避免并不能克服的客观情况。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；也可以是社会现象、社会异常事件或者政府行为，如合同订立后政府颁发新的政策、法律和行政法规，致使合同无法履行，再如战争、罢工、骚乱等社会异常事件。

在数字证书认证活动中，DFCA 由于不可抗力因素而暂停或终止全部或部分证书服务的，可根据不可抗力的影响而部分或者全部免除违约责任。其他认证各方（如订户）不得提出异议或者申请任何补偿。

9.17 其他条款

DFCA 对本 CPS 拥有最终解释权。