

中国移动 CMCA 电子认证业务规则

<版本：V1.0>

生效日期：2016 年 9 月 29 日

卓望数码技术（深圳）有限公司

文档版本控制表			
名称及版本	主要修改说明	完成时间	修改人
V0.1	正式发布	2010.7.1	委员会 工作组
V0.1A	根据 CMCTN 证书策略修订本 CPS，主要修订章节为：1.4.2 证书类型和应用范围，对移动特色证书类型及其相应的安全策略、应用场景进行补充说明	2010.9.10	委员会 工作组
V0.1B	根据工信部运营资质预审会议专家意见修订，主要修订章节为：4.1 证书申请；4.2.3 证书申请处理的时间；4.10/4.11 证书挂起/证书解挂，补充处理时间 5.2.1 可信角色；补充增加章节：4.9.10CA 证书吊销列表的发布；6.6 系统生命周期控制	2010.11.20	委员会 工作组
V1.0	修改 5.1.3 温度，湿度描述：温度控制范围在 18℃~28℃，湿度控制范围在 30%~75%RH	2016.9.29	委员会 工作组

目　录

1. 概括性描述 1

1.1 概述 1
1.2 文档名称与标识 2
1.2.1 名称 2
1.2.2 版本 2
1.3 电子认证活动参与者 2
1.3.1 电子认证服务机构 2
1.3.2 注册机构（RA） 3
1.3.3 受理点（LRA） 3
1.3.4 订户 4
1.3.5 依赖方 4
1.3.6 其他参与者 4
1.4 证书应用 4
1.4.1 适合性 4
1.4.2 证书类型和应用范围 5
1.4.3 限制的证书应用 8
1.4.4 受禁的证书应用 9
1.5 策略管理 9
1.5.1 策略文档管理机构 9
1.5.2 联系人 9
1.5.3 决定 CPS 符合策略的机构 9
1.5.4 CPS 批准程序 10
1.6 定义和缩写 10

2. 信息发布与信息管理 11

2.1 信息库 11
2.2 信息发布 11
2.2.1 CPS 的发布 11
2.2.2 公众信息的发布 12
2.2.3 认证信息的发布 12
2.3 发布的时间或频率 12
2.4 信息库访问控制 12

3. 身份标识与鉴别 14

3.1 命名 14
3.1.1 名称类型 14
3.1.2 对名称有意义的要求 14
3.1.3 订户的匿名或伪名 15
3.2 初始身份确认 15
3.2.1 证明拥有私钥的方法 15
3.2.2 组织机构身份的鉴别 15

3.2.3 个人身份的鉴证 16
3.2.4 设备身份的鉴证 17
3.2.5 代码身份的鉴证 18
3.2.6 账号证书的身份鉴证 18
3.2.7 手机号码的鉴别 19
3.3 更新请求的标识与鉴别 19
3.3.1 常规更新的标识与鉴别 19
3.3.2 吊销后更新的标识与鉴别 20
3.4 吊销请求的标识与鉴别 20
3.4.1 证书吊销情况 20
3.4.2 吊销操作 21
3.4.3 吊销申请的确认 21
4. 证书生命周期操作要求 22
4.1 证书申请 22
4.1.1 证书申请实体 22
4.1.2 注册过程与责任 23
4.1.3 证书申请流程 24
4.2 证书审核 26
4.2.1 执行识别与鉴别功能 26
4.2.2 证书申请批准和拒绝 26
4.2.3 处理证书申请的时间 26
4.3 证书签发 26
4.3.1 签发证书 26
4.3.2 拒绝签发证书 27
4.4 证书接受 27
4.4.1 证书接受 27
4.4.2 证书申请者的承诺 27
4.4.3 证书申请者的责任 28
4.4.4 证书的发布 29
4.5 密钥和证书的使用 29
4.5.1 订户私钥和证书的使用 29
4.5.2 依赖方公钥和证书的使用 29
4.5.3 密钥和证书使用的相关责任 30
4.6 证书更新 30
4.6.1 证书更新的原因 30
4.6.2 请求证书更新的实体 30
4.6.3 证书更新流程 30
4.6.4 对更新证书的发布 32
4.7 证书密钥更新 32
4.7.1 密钥更新的原因 32
4.7.2 请求密钥更新的实体 32
4.7.3 密钥更新的流程 33
4.7.4 对更新证书的发布 33

4.8 证书变更 33
4.8.1 证书变更的原因 33
4.8.2 请求证书变更的实体 33
4.8.3 证书变更的流程 33
4.8.4 对变更后新证书的发布 33
4.9 证书吊销 34
4.9.1 证书吊销的原因 34
4.9.2 请求证书吊销的实体 34
4.9.3 吊销请求的流程 35
4.9.4 吊销请求宽限期 35
4.9.5 电子认证服务机构处理吊销请求的时限 35
4.9.6 依赖方检查证书吊销的要求 35
4.9.7 CRL 发布频率 36
4.9.8 在线状态查询要求 36
4.9.9 证书吊销的注意事项 36
4.9.10 CA 证书吊销列表的发布周期 36
4.10 证书挂起 37
4.10.1 证书挂起的原因 37
4.10.2 请求证书挂起的实体 37
4.10.3 挂起请求的流程 37
4.10.4 挂起的期限限制 37
4.11 证书解挂 38
4.11.1 证书解挂的原因 38
4.11.2 请求证书解挂的实体 38
4.11.3 证书解挂的流程 38
4.12 密钥恢复 39
4.12.1 密钥恢复的原因 39
4.12.2 请求密钥恢复的实体 39
4.12.3 密钥恢复的流程 39
4.12.4 密钥恢复的注意事项 39
4.13 证书状态服务 40
4.13.1 CRL 40
4.13.2 OCSP 40
4.14 CA 服务终止 40
4.15 密钥生成、备份与恢复 40
4.15.1 加密密钥生成、备份与恢复 40
4.15.2 注意事项 41
5. 认证机构设施、管理和操作安全控制 42
5.1 物理安全控制 42
5.1.1 物理场地安全 42
5.1.2 物理访问 43
5.1.3 电力与空调 43
5.1.4 水患防治 44

5.1.5 火灾防护 44
5.1.6 介质存储 44
5.1.7 废物处理 44
5.1.8 异地备份 44
5.2 流程安全控制 45
5.2.1 可信角色 45
5.2.2 每项任务需要的人数 45
5.2.3 安全令牌控制 46
5.2.4 职责分割原则 46
5.3 人员控制 47
5.3.1 资格、经历和无过失要求 47
5.3.2 背景审查程序 47
5.3.3 培训要求 47
5.3.4 再培训周期和要求 48
5.3.5 岗位分离和轮换 48
5.3.6 未授权行为的处罚 48
5.3.7 提供给员工的文档 48
5.4 安全审计 49
5.4.1 记录事件的类型 49
5.4.2 处理日志的周期 50
5.4.3 审计日志的保存期限 50
5.4.4 审计日志的保护 50
5.4.5 审计日志备份程序 51
5.4.6 审计收集系统 51
5.4.7 对导致事件实体的处理 51
5.4.8 脆弱性评估 51
5.5 记录归档 52
5.5.1 归档记录的类型 52
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 52
5.5.5 记录时间戳要求 53
5.5.6 归档收集系统 53
5.6 密钥更替 53
5.6.1 密钥更替定义 53
5.6.2 根证书有效期 53
5.6.3 CRL 54
5.7 损害与灾难恢复 54
5.7.1 事故和损害处理程序 55
5.7.2 计算资源、软件和/或数据的损坏 55
5.7.3 实体私钥损害处理程序 55
5.7.4 灾难后的业务连续性能力 56
5.8 电子认证服务机构或注册机构的业务终止 56

5.8.1 CA 终止原因 56
5.8.2 终止通知 56
5.8.3 终止归档 56
5.8.4 终止措施 56
5.8.5 RA 的终止 57

6. 认证系统技术安全控制 58

6.1 密钥对的生成和安装 58
6.1.1 CA 密钥对的产生 58
6.1.2 订户密钥对的生成 58
6.1.3 私钥传送 59
6.1.4 公钥传送 59
6.1.5 电子认证服务机构公钥传送 59
6.1.6 密钥的长度 60
6.1.7 公钥参数的生成 60
6.1.8 密钥用途 60
6.2 私钥保护和密码模块工程控制 61
6.2.1 密码模块的标准和控制 61
6.2.2 私钥多人控制 61
6.2.3 私钥托管 62
6.2.4 私钥备份 62
6.2.5 私钥归档 62
6.2.6 私钥导入、导出密码模块 62
6.2.7 私钥在密码模块的存储 62
6.2.8 激活私钥 62
6.2.9 解除私钥激活状态 63
6.2.10 销毁私钥 63
6.3 密钥对管理的其他方面 64
6.3.1 公钥归档 64
6.3.2 证书操作期和密钥对使用期 64
6.4 敏感数据 64
6.4.1 敏感数据的产生 64
6.4.2 敏感数据的保护 64
6.5 计算机安全控制 65
6.5.1 计算机安全技术要求 65
6.5.2 计算机安全评估 65
6.6 系统生命周期控制 65
6.6.1 系统开发控制 65
6.6.2 安全管理控制 66
6.6.3 生命周期的安全控制 66
6.7 网络的安全控制 66
6.8 时间戳 66

7. 证书、证书吊销列表和在线证书状态协议 67

7.1 证书 67
7.1.1 版本号 *67*
7.1.2 证书标准项 *67*
7.1.3 证书扩展项 *68*
7.1.4 密钥算法对象标识符 *71*
7.1.5 名称格式 *71*
7.2 证书吊销列表 71
7.2.1 版本号 *71*
7.2.2 CRL 和 CRL 条目扩展项 *71*
7.3 在线证书状态查询协议 72

8 认证机构审计和其他评估 73

8.1 审计的频率或情形 73
8.1.1 中国移动 CMCA 的审计 *73*
8.1.2 中国移动 CMCA 对关联单位的审计 *73*
8.2 审计者的资质 73
8.3 审计者与中国移动 CMCA 的关系 74
8.3.1 审计者与中国移动 CMCA 的关系 *74*
8.3.2 审计报告与中国移动 CMCA 的关系 *74*
8.4 审计内容 74
8.5 对问题与不足采取的措施 75
8.6 评估结果的传达与发布 75

9 法律责任和其他业务条款 75

9.1 费用 75
9.1.1 证书费用 *75*
9.1.2 退款策略 *75*
9.2 财务责任 76
9.2.1 保险范围 *76*
9.2.2 对最终实体的保险或担保 *76*
9.3 业务信息保密 76
9.3.1 保密信息范围 *76*
9.3.2 不属于保密的信息 *77*
9.3.3 对业务信息保密的责任 *77*
9.4 个人隐私保密 78
9.4.1 隐私保密方案 *78*
9.4.2 作为隐私处理的信息 *78*
9.4.3 不被视为隐私的信息 *78*
9.4.4 保护隐私的责任 *78*
9.4.5 依法律或行政程序的信息披露 *78*
9.4.6 其他信息披露情形 *79*
9.5 知识产权 79
9.6 陈述与担保 79
9.6.1 电子认证服务机构的陈述与担保 *79*

9.6.2 注册机构的陈述与担保 *80*
9.6.3 订户的陈述与担保 *80*
9.6.4 依赖方的陈述与担保 *81*
9.6.5 其他参与者的陈述与担保 *81*
9.7 担保免责 81
9.8 有限责任 82
9.9 赔偿 82
9.9.1 赔偿条件 *82*
9.9.2 赔偿限制 *83*
9.9.3 其他机构赔偿 *84*
9.10 有效期限与终止 84
9.11 修订 85
9.12 争议处理 85
9.13 管辖法律 85
9.14 适用的法律 85
9.15 一般条款 86
9.15.1 完整协议 *86*
9.15.2 转让 *86*
9.15.3 分割性 *86*
9.15.4 不可抗力 *86*
9.16 其他条款 87

1. 概括性描述

1.1 概述

中国移动数字证书认证中心（简称中国移动CMCA）由卓望数码技术（深圳）有限公司组建并负责运营，是一个面向全国、面向社会提供第三方电子认证服务的电信级运营机构，为传统互联网、移动互联网的各类实体建立信任关系，保证实体身份的真实性，为信息的保密性、完整性以及关键操作的不可抵赖性提供全面的服务。

在技术体系上，中国移动CMCA具备一套技术先进，能满足客户应用需求、实用、开放、遵循标准并具有强大的处理能力的PKI系统；在业务应用上，中国移动CMCA能够全面支持传统互联网和移动网络上的多种证书应用和安全解决方案。

本业务规则根据国家相关法律法规的要求，详细阐述了中国移动CMCA开展认证业务的各项规范、流程和保障措施，以及电子认证服务参与各方所承担的责任与义务，中国移动CMCA及其授权注册机构（RA）和业务受理点（LRA）必须遵循本业务规则中的各项规范。中国移动CMCA电子认证服务体系内的实体，包括中国移动CMCA数字证书订户，在参与电子认证服务前有义务了解本业务规则所规定的条款，承担相应的责任和业务，并据此监督中国移动CMCA及其授权注册机构和业务受理点的规范运营。

本CPS的总体条款结构符合工业和信息化部所发布的《电子认证业务规则规范（试行）》，并在制定过程中参照《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务机构年度检查指引（试行）》及国家密码主管部门相关标准制定。在不改变《电子认证业务规则规范（试行）》总体框架的情况下，在制定本CPS时可能会对该框架进行扩充，以适应中国移动CMCA认证业务的特定需求。

本CPS（V1.0）的生效日期是**2016年9月29日**。

1.2 文档名称与标识

1.2.1 名称

本文档中文名称为《中国移动数字证书认证中心电子认证业务规则》（简称《中国移动 CMCA 电子认证业务规则》），也被称为中国移动 CMCA 电子认证业务声明，英文名称为 Certification Practice Statement（简称 CPS）。

1.2.2 版本

本 CPS 为中国移动 CMCA 发布的第 4 个版本，为中国移动 CMCA CPS 1.0 版本，即版本号为 V1.0。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

电子认证服务机构指的是证书认证机构，是颁发证书的实体，即中国移动数字证书认证中心。电子认证服务机构应承担的责任和业务是：

1) 保证 CA 机构使用和发放的公钥算法在现有技术条件下不会被攻破；
2) 保证 CA 机构本身的签名私钥在中国移动 CMCA 内部得到安全的存放和保护；
3) 保证 CA 建立和执行的安全机制符合国家政策的规定；
4) 除上述规定的职责条款，CA 机构、CA 的服务机构、CA 的受理点、CA 的雇员不承担其它任何义务。

中国移动 CMCA 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损失、损坏或赔偿责任。这些事件包括罢工或其他劳动纠纷、暴动、国内骚动、供应商故意或无意的行为、不可抗力、战争、火灾、爆炸、地震、洪水或其他大灾难。

由于技术的进步与发展，中国移动 CMCA 会要求订户及时更换密钥或证书

以保证中国移动 CMCA 能更好地履行职责。

1.3.2 注册机构（RA）

注册机构也称为注册审核机构，是为最终证书申请者建立注册过程的实体，对证书申请者进行身份鉴别和标识，发起或传递证书吊销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。

作为中国移动 CMCA 机构授权委托的下属机构，RA 负责证书客户信息的审核、整理汇总、统计分析，与上级 CA 进行数据交换，管理和服务下层注册分支机构和下层受理点。

RA 有责任妥善保存客户的数据，不允许将客户的数据透露给与证书申请无关的任何单位或个人，不允许用作商业利益方面的用途。

中国移动 CMCA 机构除承担 CA 的角色外，也承担部分 RA 的角色，同时，可授权委托其他机构承担 RA 角色。地区、行业、机构均可以申请成为中国移动 CMCA 的注册机构。

1.3.3 受理点（LRA）

RA 可以根据业务发展需要，遵循中国移动 CMCA 认证体系地域或行业的划分情况，授权建立相应的受理点或注册分支机构（LRA）。

LRA 需经过中国移动 CMCA 审查，中国移动 CMCA 授权特定单位或实体，负责办理和审批数字证书申请。数字证书申请手续、过程和要求，必须与中国移动 CMCA 正在实施的电子认证业务规则（CPS）以及中国移动 CMCA 的 CA 受理点授权协议书相一致。

受理点负责向中国移动 CMCA 或经中国移动 CMCA 授权的注册机构或注册分支机构提供证书申请实体的信息，包括申请实体的名称、可以表明身份的证件号码和联系方法（通信地址、电子邮件信箱、电话等）。受理点根据这些信息为申请实体制作证书或根据申请实体的要求，提供申请实体自行申请的技术支持。

1.3.4 订户

中国移动 CMCA 订户即证书所有人，包括所有由 CMCA 颁发证书的最终用户。订户是一个实体，可以是个人、机构、或设备（如防火墙、路由器、可信服务器、或在机构中用于安全通信的其他设备）。

一般情况下，证书是直接颁发给个人或机构由其自己使用。但是，总存在其他情形，需要证书的一方与申请证书的实体不同，例如一个组织可能为其雇员请求证书，或者为其 Web 服务器申请证书。当出现这种情况时，本 CPS 采用两个术语进行区分：“订户”特指与认证机构或注册机构签订合同购买证书的实体；“主体”特指证书中主体域所标识的实体。从这个角度看，订户一定是人或组织机构的授权代表，而主体则有可能是设备。

1.3.5 依赖方

依赖方是为某一应用而使用、信任中国移动 CMCA 机构或其注册机构签发的证书的个人或组织。依赖方可以是中国移动 CMCA 的证书订户，也可以不是订户。

依赖方享有相应的利益，包括中国移动 CMCA 可能提供的证书保障，以及中国移动 CMCA 认证业务声明或证书策略中涉及的权益。

1.3.6 其他参与者

为以上未提及的隶属于中国移动 CMCA 证书体系的实体。如目录服务提供者、以及其他提供电子认证相关服务的实体。

1.4 证书应用

1.4.1 适合性

CA 证书从功能适用下列安全需要：

1) 身份认证：保证采用中国移动 CMCA 认证的证书持有者身份的合法性。

2) 验证信息完整性：保证采用中国移动 CMCA 数字证书和数字签名时，可以验证信息在传递过程中是否被篡改，发送和接收的信息是否完整一致。

3) 验证数字签名：是信任体交易的不可抵赖性的依据。必须指出，对于任何电子通信或交易，不可抵赖性应根据法律和争议解决办法裁定。

1.4.2 证书类型和应用范围

中国移动 CMCA 可为传统互联网应用如电子政务、电子商务、电子办公等应用领域提供电子认证服务，但与此同时，中国移动 CMCA 的主要证书应用集中在移动电子商务以及移动互联网应用领域。从证书介质类型来看，除传统 CA 主流证书介质 USBKEY 外，中国移动 CMCA 证书主要以手机卡介质为主。

为清晰描述中国移动 CMCA 证书类型、应用范围及其相应的安全策略，我们将中国移动 CMCA 证书分成两大类，即基线证书（标准数字证书）与扩展证书（移动特色证书），分别遵循中国移动证书信任体系（CMCTN）的基线证书策略与扩展证书策略。

1.4.2.1 扩展证书

1) 手机号码证书

此类证书是中国移动 CMCA 为移动手机用户提供的扩展数字证书

- 该证书与移动用户手机号码唯一绑定
- 证书载体支持 USBKEY、智能卡、手机 SIM 卡
- 应用范围主要为民生便捷应用，非接触刷卡应用，如小额手机支付、积分消费、手机电子票、手机邮箱等，同时该证书还可提供身份认证登录等互联网应用服务
- 安全策略：此类证书根据应用场景的便捷性要求，不对手机用户做实名身份认证，但必须验证用户手机号码的有效性

2) 手机实名证书

此类证书是中国移动 CMCA 为移动手机用户（个人）提供的扩展数字证书

- 该证书与移动手机用户实名身份、手机号码进行绑定

- 证书载体支持智能卡、手机 SIM 等
- 支持高端移动电子商务应用，如大额手机支付、高端 VIP 会员服务、高端安全邮件服务、手机银行服务等，还可提供实名互联网认证登录、电子签名/签章等互联网应用服务
- 安全策略：此类证书将对手机用户（个人）进行严格的实名身份认证并验证其手机号码的有效性，用户可以通过中国移动营业厅等服务渠道进行实名登记认证。

3) 移动终端设备证书

此类证书是中国移动 CMCA 为移动手机用户提供的扩展数字证书

- 该证书与终端设备通信属性（如手机 SIM 卡）唯一绑定
- 证书载体为终端设备或手机 SIM 卡
- 主要颁发给需要安全鉴别的移动终端设备，可用于数据加解密和信息签名，以实现移动终端设备通信的信息保密及提供信息源发性证明、完整性保障
- 安全策略：此类证书根据应用场景的便捷性要求，不对终端设备的实体做实名身份认证，但须验证手机终端设备属性

4) 终端应用开发者标识证书

此类证书是中国移动 CMCA 为手机终端应用开发者提供的扩展数字证书。

- 开发者可以为企业开发者或个人开发者
- 证书载体支持 USBKEY、智能卡、手机 SIM 卡等
- 用于中国移动对终端应用开发者真实身份的有效认证，开发者可用证书对其开发的终端应用软件进行可靠签名。与普通代码签名证书不同，终端应用开发者标识证书对通过中国移动渠道发布的终端应用提供开发者著作权声明保护以及终端应用责任追溯机制。
- 安全策略：此类证书将对开发者个人或企业进行严格的实名身份认证，个人开发者将按照个人类实名审核要求进行身份鉴证，企业开发者江按照企业类实名审核要求进行身份鉴证。

5) 终端应用标识证书

此类证书是中国移动 CMCA 为依据终端应用机制发布的终端应用提供的扩

展数字证书。

- 应用为适用于手机、电子设备等终端的工具、软件、游戏等应用
- 用于标识经过中国移动终端应用测试认证中心按照终端应用规范测试通过的应用，终端应用认证中心对通过测试的应用适用颁发给该应用的终端应用标识证书进行有效的电子签名。符合中国移动终端应用认证机制的终端设备通过对终端应用标识证书签名的验证，可以实现对应用使用的终端能力进行有效控制，并确保只有经过中国移动终端应用测试认证中心测试的应用才能安装和使用，从而有效的保障中国移动用户使用安全绿色的终端应用。
- 安全策略：此类证书为中国移动终端应用认证中心向中国移动CMCA通过专用接口申请的应用标识证书，中国移动CMCA需要严格鉴证中国移动终端应用认证中心的身份。

1.4.2.2 基线证书

1) 账号证书：客户使用此证书标识特定应用场景中的虚拟身份，不进行实名认证，如邮件证书证书等，也称为非实名制证书。账号证书的订户通常是个人；

   安全策略：此类证书并非CMCA主要的证书类型，对于此类证书的颁发对象实体，CMCA不进行实名身份认证

2) 个人证书：也可称为自然人证书，客户使用此证书来向对方表明个人的身份，同时应用系统也可以通过证书获得客户的其他身份信息，可用于：身份识别、文档签名、交易签名、敏感操作签名和信息申报等

   安全策略：CMCA将对个人实名身份进行严格的审核鉴证，鉴证通过后才予以签发证书。

3) 企业证书：颁发给独立的单位、组织，在互联网上证明该单位、组织的身份，也可称为单位证书、机构证书。可用于：身份识别、文档签名、交易签名、票据签名和信息申报等业务。

   安全策略：CMCA将对单位、组织的实名身份进行严格的审核鉴证，鉴证通过后才予以签发证书。

4) 服务器证书：主要颁发给需要安全鉴别的服务器设备，还可用于数据加解密和信息签名，以实现信息保密及提供信息源发性证明、完整性保障。**安全策略：CMCA 将对服务器持有人，如企业单位或个人的实名身份进行严格的审核鉴证，鉴证通过后才予以签发证书。**

5) 代码签名证书：代码签名证书颁发给个人或者具有企业身份的软件开发商和提供商，通过对其提供的软件代码进行数字签名，可以有效防止该软件代码被篡改，并且能够保护软件开发商的版权利益。当客户在网上下载经过代码签名的软件时，将会得到提示，从而确认软件的来源真实性、可靠性，以及软件从签名到下载前，未遭到修改或破坏。

安全策略： CMCA 将对软件开发商即代码持有人 持有人，如企业单位或个人的实名身份进行严格的审核鉴证，鉴证通过后才予以签发证书。

另外，中国移动 CMCA 向内部客户、内部或合作伙伴的开发测试人员提供测试证书，可向中国移动 CMCA 直接向申请，测试证书仅用于申请时审核的有效期和应用范围内使用，且中国移动 CMCA 不承担测试证书的法律责任，本 CPS 将不对测试证书进行描述。

1.4.3 限制的证书应用

证书禁止在任何违反国家法律、法规或破环国家安全的情形下使用，否则由此造成的法律后果由客户自己承担。

中国移动 CMCA 所颁发的某些证书在功能上是受到限制的，如个人证书只能用于个人订户的应用，而不能作为服务器证书或企业证书使用。企业证书只能用于代表组织机构的场合。

证书的密钥用法扩展项中限制了与证书中公钥对应私钥的使用目的，如最终客户证书不能作为 CA 证书使用。这种限制是由基本限制扩展项缺省值确定的。然而，基于扩展项的限制的有效性取决于软件，如果有关软件不遵守有关约定，其对证书的使用将超出本 CPS 限定的应用范围，将是不受保护的。

1.4.4 受禁的证书应用

中国移动 CMCA 所签发的证书在下列情况下禁止应用：

1、由于证书的使用可能导致人员死亡、伤残的情形。

2、由于证书的使用可能导致环境破坏的情形。

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 由卓望数码技术（深圳）有限公司成立的中国移动 CA 中心制定，并由该中心下设的安全认证策略管理委员会进行管理。

1.5.2 联系人

中国移动 CMCA 将对 CPS 进行严格的版本控制和文档管理，由中国移动 CMCA 安全认证策略管理委员会负责管理，由专门的 CPS 管理人员负责日常维护，指定运营服务部负责对外联络。

联系部门：中国移动 CA 中心运营服务部门

电话：86-755-66820666

传真：86-755-66820001

地址：深圳高新技术产业园区南区深港产学研基地大楼六楼

电子邮件：caservice@aspire-tech.com

1.5.3 决定 CPS 符合策略的机构

卓望数码技术（深圳）有限公司中国移动 CA 中心安全认证策略管理委员会对本 CPS 文件具有决定权和最终解释权。

1.5.4 CPS 批准程序

在中国移动 CMCA 认证业务声明做出任何变动之前，中国移动 CMCA 安全认证策略管理委员会将对提供的变动建议进行研究，做出变更决定。根据具体修订变更需求和内容，中国移动 CMCA 会征求内部、外部专家和律师顾问等专业人士的意见，通过安全策略管理委员会审批形成最终修订决议。中国移动 CMCA 将在决议形成后，在中国移动 CMCA 网站正式公布变更后的中国移动 CMCA 电子认证业务规则文档。

1.6 定义和缩写

CMCTN	中国移动证书信任体系 (China Mobile Ceritificate Trust Network)
CP	证书策略 (certification policy)
CPS	电子认证业务规则或电子认证业务说明 (certification practice statement)
CRL	证书吊销列表或证书黑名单 (certificate revocation list)
CSR	证书签名请求 （*Certificate Signing Request*）
HTTP	超文本传输协议 (Hypertext Transfer Protocol)
HTTPS	安全套接层下的超文本传输协议 (Hypertext Transfer Protocol with SSL)
CA	电子认证服务机构 (certificate authority)
RA	注册机构 (registration authority)
LRA	本地注册受理点或本地受理点 (local registration authority)
PIN	个人授权码 (personal identification number)
OCSP	在线证书状态查询协议 (online certificate search protocol)
LDAP	轻量目录访问协议 (Lightweight Directory Access Protocol)
PKCS	公共密钥加密标准 （*Public Key Cryptography Standards*）
PKI	公共密钥基础设施 (public key infrastructure)
SSL	加密套阶字协议层 （*Secure Sockets LRAyer*）

URL	指定的信息位置 （*uniform resource locator*）
WWW or Web	万维网 （World Wide Web）
X.509	国际电信同盟认证体系的证书标准 （the ITU-T standard for certificates and their corresponding authentication framework）

2. 信息发布与信息管理

2.1 信息库

中国移动 CMCA 认证信息发布的信息库包括中国移动 CA 中心的 WWW 网站、WAP 网站、认证系统的证书服务站点、LDAP、CRL 及 OCSP 服务器等。另外，中国移动 CMCA 授权的注册机构的证书服务站点也是认证信息发布的信息库。

2.2 信息发布

2.2.1 CPS 的发布

中国移动 CMCA 认证业务规则由卓望数码技术（深圳）有限公司设立的中国移动 CA 中心完全拥有，并负责本规则的解释，一经中国移动 CMCA 在网站或以书面声明形式发布、更改，即时生效，并对一切仍有效的数字证书的使用者、新的数字证书及相关业务的申请者、认证体系相关实体均具备约束力。

本业务规则的修订与发布一律须经中国移动 CMCA 的核准和正式发布。

本 CPS 通过以下几种方式发布：

- 以电子的方式，在中国移动 CMCA 网站的信息库中发布，网站地址：www.cmca.net
- 通过电子邮件发布，电子邮箱地址 caservice@ aspire-tech.com

2.2.2 公众信息的发布

中国移动 CMCA 将及时在网站上公布相关的公众信息。

2.2.3 认证信息的发布

证书在签发成功后，中国移动 CMCA 自动将证书副本发布到目录服务器上。

中国移动 CMCA 定期公布的证书有效期内被废止的数字证书可从中国移动 CMCA 的 CRL 发布站点获取。

证书客户可以在中国移动 CMCA 的网站中查询获得其证书有关信息。

2.3 发布的时间或频率

中国移动 CMCA 有权利对其 CPS 进行改动和版本升级，其发布时间及频率由中国移动 CMCA 决定，中国移动 CMCA 会在网站上发布最新版本 CPS，证书相关方可通过中国移动 CMCA 信息库 7x24 小时获取 CPS。

中国移动 CMCA 的网站实时更新，会在第一时间发布和证书业务相关的信息。

中国移动 CMCA 的目录服务器上每日更新目录，通常在 24 小时内自动发布最新证书吊销列表 CRL，发布时间为每天的凌晨，也可人工发布最新 CRL。证书客户可在中国移动 CMCA 网站上查询、下载数字证书以及 CRL。

2.4 信息库访问控制

2.2 节中所发布信息的查询、获取是公开的，没有任何限制。

中国移动 CMCA 将及时在网站上公布新的信息，并且只有中国移动 CMCA 有权对网站上的信息进行更新和处理。

中国移动 CMCA 设置了信息访问控制和安全审计措施，保证只有经过授权的中国移动 CMCA 工作人员才能编写和修改中国移动 CMCA 在线的公告版本和公布信息。

中国移动 CMCA 在必要时可自主选择是否实行信息的权限管理，以确保只

有证书客户才有权阅读受中国移动 CMCA 控制的信息资料。

3. 身份标识与鉴别

3.1 命名

3.1.1 名称类型

中国移动 CMCA 证书符合 X509.3 标准，甄别名格式遵守 X501 标准。

根据证书主体类型不同，中国移动 CMCA 签发的证书的主体名字可以是人员姓名、组织机构名、部门名、域名等，为保护用户隐私，手机号码证书的主体名称定义为可识别名称的散列值。

甄别名包含于每张证书的主题中，唯一标识证书客户的身份。

每个证书持有者将对应至少一个可分辨的甄别名 DN（X.500 中的 DN）。

甄别名 DN 必须对中国移动 CMCA 所有证书持有者都是唯一的。中国移动 CMCA 接受唯一的甄别名，可根据 DN 鉴别证书持有者。

中国移动 CMCA 不接受使用商标作为甄别名。

3.1.2 对名称有意义的要求

对于账号证书，出现在证书主体甄别名中的通用名称不作为标识订户的有效主体信息，不被鉴别和认证。CMCA 根据需要，可以对甄别名中的关键信息（如邮件证书中的邮件地址）进行鉴别。

个人证书主体甄别名中的通用名通常是个人的真实姓名，或者其他能唯一标识客户身份的其他信息，如个人身份证号码等，它作为标识订户的关键信息被鉴别和认证。

企业证书主体甄别名的通用名通常是组织机构的名称，或者其他能唯一标识该机构的其他信息，如组织机构代码等，它作为标识订户的主要信息同其他信息

一起被鉴别和认证。

服务器证书主体甄别名中的通用名通常是设备名、域名或为该服务器分配的IP，它作为标识订户的主要信息同其他信息（如组织机构名称）一起被鉴别和认证。

代码签名证书、终端应用开发者标识证书主体甄别名的通用名通常是组织机构的名称或者个人代码开发者姓名，它作为标识订户的主要信息同其他信息一起被鉴别和认证。

3.1.3 订户的匿名或伪名

账号证书可以使用匿名或伪名。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

中国移动 CMCA 通过使用经数字签名的 PKCS#10 格式的证书请求，验证证书申请者拥有私钥。

3.2.2 组织机构身份的鉴别

组织机构在申请企业证书、服务器证书、代码签名证书、终端应用企业开发者标识证书等机构类证书时，需要指定授权代表即经办人进行办理。该机构需要向中国移动 CMCA、RA 或 LRA 提供数字证书申请表格并加盖公章表示接受证书申请的有关条款，并承担相应的责任。

中国移动 CMCA 或其授权机构审核组织机构是否符合要求，身份鉴别方式如下：

1) 申请者需向中国移动 CMCA 提供机构确实存在的证明文件，证明文件由政府权威机关颁发，包括但不限于组织机构代码证、企业工商营业执照、税务登记证等。中国移动 CMCA 或其授权机构需审核证明文件并将复印

件进行存档。

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

3) 中国移动 CMCA 或其授权机构还需审核企业证书代表人的身份和资格，包括但不限于经办人的有效身份证件。

4) 如果中国移动 CMCA 或其授权机构已经预先明确了机构的身份，那么中国移动 CMCA 或其授权机构可以信赖这些证明。

对于机构类证书，CMCA 采用如下方法确认该组织机构知晓并授权证书申请，即代表组织机构提交证书申请的人是经过授权的：

1) 面对面验证方式；或者，

2) 使用从网络或其它常规途径获取验证电话号码，进行电话验证，获得组织机构有关申请及授权事宜的确认；或者，

3) 验证申请者是否知晓或拥有通常只有真正的申请者才知晓或拥有的秘密；或者，

4) 通过注册机构的人员检验、确认与该组织机构相关的证书申请者的身份及其证书申请行为。

3.2.3 个人身份的鉴证

自然人在申请个人证书、手机实名证书、个人服务器证书、代码签名证书、终端应用个人开发者标识证书等个人类证书时，需要向中国移动 CMCA 提供数字证书申请表格并签字表示接受证书申请的有关条款，并承担相应的责任。

中国移动 CMCA 或其授权机构审核个人是否符合要求，身份鉴别方式如下：

1) 申请者需向中国移动 CMCA 提供有效身份证明文件，包括身份证、护照、军官证等。中国移动 CMCA 或其授权机构需审核证明文件并将复印件进行存档。

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

3) 如申请者授权经办人申请数字证书，中国移动 CMCA 或其授权机构还需审核经办人的身份和资格，包括但不限于经办人的有效身份证件。

4) 如果中国移动 CMCA 或其授权机构已经预先明确了个人的身份，那么中国移动 CMCA 或其授权机构可以信赖这些证明。

对于个人类证书，CMCA 采用如下的身份验证方法：

1) 使用面对面的验证方式；或者，

2) 通过真正的申请者实名拥有的电话验证、确认其在申请证书；或者，

3) CMCA 认为的可信的第三方机构担保形式（如企业提供人员列表的同时，就提供了一定程度的第三方担保），获得组织机构有关申请及授权事宜的确认。

如个人用户申请手机用户证书，除进行以上鉴证外，中国移动 CMCA 或其授权机构还应通过手机服务密码、激活验证码等方式验证其手机号码的真实性和有效性。

3.2.4 设备身份的鉴证

服务器、移动终端设备等设备身份的鉴别会根据其拥有者的不同而有所区别，中国移动 CMCA 必须对订户进行身份鉴证，包括如下内容：

1) 设备拥有者的身份鉴别根据不同类型按照不同的身份鉴别方式执行，订户为机构的，按照本 CPS$3.2.2 节描述执行；订户为个人的，身份鉴别按照$3.2.3 节描述执行。

2) 对个人或机构对该域名的合法拥有权进行鉴别。

3) 核查证书申请除域名外的其他关键信息与有效文件或第三方数据库的资料是否相符，避免信息填写有误，但注册信息最终以申请者确认为准。

对于设备类证书，CMCA 采用如下方法确认设备拥有实体知晓并授权证书申请，即代表设备拥有实体提交证书申请的人是经过授权的：

1) 面对面验证方式；或者，

2) 使用从网络或其它常规途径获取验证电话号码，进行电话验证，获得设备拥有实体有关申请及授权事宜的确认；或者，

3) 验证申请者是否知晓或拥有通常只有真正的申请者才知晓或拥有的秘

密；或者，

4) 通过注册机构的人员检验、确认与该设备拥有实体相关的证书申请者的身份及其证书申请行为。

3.2.5 代码身份的鉴证

代码、终端应用代码等代码类身份的鉴别会根据其拥有者的不同而有所区别，中国移动 CMCA 必须对订户进行身份鉴证，包括如下内容：

1) 代码拥有者的身份鉴别根据不同类型按照不同的身份鉴别方式执行，订户为机构的，按照本 CPS$3.2.2 节描述执行；订户为个人的，身份鉴别按照$3.2.3 节描述执行。
2) 核查证书申请关键信息与有效文件或第三方数据库的资料是否相符，避免信息填写有误，但注册信息最终以申请者确认为准。
3) 中国移动 CMCA 仅根据客户要求，在正确核实申请者身份后签发代码签名证书，不对证书订户对软件代码的合法拥有权进行鉴定。

对于代码签名证书、终端应用开发者标识证书，CMCA 采用如下方法确认软件开发者知晓并授权证书申请，即代表软件开发者提交证书申请的人是经过授权的：

1) 面对面验证方式；或者，
2) 使用从网络或其它常规途径获取验证电话号码，进行电话验证，获得软件开发者有关申请及授权事宜的确认；或者，
3) 验证申请者是否知晓或拥有通常只有真正的申请者才知晓或拥有的秘密；或者，
4) 通过注册机构的人员检验、确认与该软件开发者相关的证书申请者的身份及其证书申请行为。

3.2.6 账号证书的身份鉴证

对于账号证书的申请，中国移动 CMCA 通过确认证书中唯一标识该证书实体的关健信息的有效性，实现对证书申请者的鉴别。

针对邮件证书，中国移动 CMCA 向证书申请中提交的、需要绑定的电子邮箱发送确认信息，以确认电子邮箱地址是真实的、正确的，验证是邮箱拥有者本人在申请证书，但中国移动 CMCA 不确认、不担保签发的证书中除电子邮箱地址以外的其他身份信息是真实的、可靠的、属于申请者本人的。

3.2.7 手机号码的鉴别

中国移动 CMCA 或其授权机构通过手机发送激活验证码或验证手机服务密码等方式验证其手机号码的真实性和有效性。

3.3 更新请求的标识与鉴别

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。中国移动 CMCA 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”。然而，在某些情况下，中国移动 CMCA 允许订户为一个现存的密钥对申请一个新证书，称作“证书更新”。对于密钥更新而言，订户证书除公钥、有效期和序列号改变外，其他信息都没改变；对于证书更新而言，和密钥更新相比，订户证书公钥也不改变。

密钥更新和证书更新与申请一个新证书在技术上是不同的。在申请一个新证书时，证书订户需到中国移动 CMCA 或其注册机构的证书服务站点，或 LRA 服务点办理业务，填写必要的申请信息；而对于密钥更新和证书更新，订户虽然同样需要访问中国移动 CMCA 或其注册机构的证书服务站点的相应服务网页，或到 LRA 现场办理，但客户无需填写申请信息，系统会自动获取订户的有关信息。

对于中国移动 CMCA 的证书认证业务，在证书有效期到期前只能通过密钥更新或证书更新签发具有相同签发者、主体名和证书用途的证书。除非先将证书吊销，否则在证书有效期到期前，不能通过申请新证书的方法获得具有相同签发者、主体名和证书用途的证书。

3.3.1 常规更新的标识与鉴别

由于证书到期、证书信息更改或密钥更新等情况，证书需要更新。

经中国移动 CMCA 签发的客户证书有效期一般为 1-3 年。证书到期前一个月，中国移动 CMCA 会提醒证书持有者进行证书更新。

证书客户申请更新证书时，填写证书更新表，按照初始身份验证步骤提交相关资料（同 3.2），并由中国移动 CMCA 或其授权机构审核。

中国移动 CMCA 或其授权机构的审核人员合理、审慎地核对申请资料的原件与复印件，根据审核人员的管理规定对申请者的资料的真实性进行表面审查，并进行批准或拒绝的操作。

3.3.2 吊销后更新的标识与鉴别

由于证书密钥泄漏或证书过期等原因，证书被吊销，证书吊销完成后不能更新证书，只能重新签发证书，其操作与证书申请相同。

3.4 吊销请求的标识与鉴别

3.4.1 证书吊销情况

- 证书的私钥泄漏
- 在证书有效期内客户终止使用证书
- 客户未缴纳证书相关费用
- 其他中国移动 CMCA 认为有必要吊销客户证书的原因

当证书私钥泄露等安全问题时，证书订户应该及时主动向中国移动 CMCA 申请作废其数字证书。中国移动 CMCA 机构和中国移动 CMCA 受理点对证书的作废请求需要予以验证。

在中国移动 CMCA 的证书业务中，证书吊销请求可以来自订户，也可以来自中国移动 CMCA 或其注册机构。证书吊销的方式可以是订户自己吊销，也可以由订户要求中国移动 CMCA 或其注册机构管理员吊销，中国移动 CMCA 和其注册机构在认为必要的时候，有权发起吊销订户证书。

3.4.2 吊销操作

证书客户申请吊销证书时，填写证书吊销申请表，通过一定的方式，如邮寄、邮件、传真等，向中国移动CMCA或其授权机构提交，并由中国移动CMCA或其授权机构审核。

3.4.3 吊销申请的确认

中国移动CMCA或其授权机构的审核人员合理、审慎地核对申请资料的原件与复印件，根据审核人员的管理规定对申请者的资料的真实性进行表面审查，并进行批准或拒绝的操作。

4. 证书生命周期操作要求

中国移动CMCA授权的注册机构提供数字证书授权、申请、发放、查询和管理等服务，提供网络安全及身份认证、电子签名验证、密钥管理等与数字证书密切相关的配套服务。本章节描述的证书包括CA 证书、RA 证书、终端客户证书。本章节主要以终端客户中的证书申请者为模板，描述证书业务规范。

4.1 证书申请

申请者必须真实填写证书申请信息，否则中国移动CMCA有权拒绝签发证书、停止证书的使用、废止证书。中国移动CMCA不承担由此造成的后果。

4.1.1 证书申请实体

证书申请者可包含个人、企业单位、事业单位、社会团体等各类组织机构、CA、RA、LRA机构以及CA 机构或RA 机构的系统及相应的管理员.

任何希望拥有账号证书的订户都可按照本业务规则要求申请账号证书。

任何需要在各类应用中采用数字证书进行真实身份标识和鉴别，实现信息保密，并提供信息源发性证明、完整性保障和抗抵赖的个人或机构，都可以申请个人证书或企业证书。

服务器证书由域名、IP地址拥有机构，或获得域名使用授权的机构中的授权人申请，其他设备证书由设备拥有者申请。

任何软件开发商或拥有软件代码版权的机构都可申请代码签名证书。

手机用户可以申请手机号码证书、手机实名证书以及移动终端设备证书，任何终端应用开发商都可以申请终端应用开发者标识证书和终端应用标识证书。

4.1.2 注册过程与责任

证书申请者可到中国移动 CMCA 注册中心及受理点申请各类证书。

对于账号证书，注册时申请者须正确填写证书实体关键信息（如电子邮件地址）。

对于企业证书，注册时申请者须正确填写以下信息：

- 机构的真实身份标识信息，包括机构法定名称、组织机构代码等；
- 机构授权的联系人信息，如姓名、电话、邮件地址等；

对于个人证书，注册时申请者须正确填写以下信息：

- 个人的真实身份标识信息，包括真实姓名、身份证号码等；
- 其他信息，如邮件地址等；

对于服务器证书，注册时申请者须正确填写以下信息：

- 服务器主机名、域名、IP 地址或设备名称及所有者信息等；
- 申请人信息，如单位名称/姓名、电话、邮件地址等。

对于代码签名证书，注册时申请者须正确填写以下信息：

- 申请人为机构：按照企业证书信息填写；
- 申请人为个人：按照个人证书信息填写；

对于手机号码证书，注册时申请者须正确以下信息：

- 手机号码：中国移动 CMCA 通过动态密码或手机服务密码等机制验证手机号码的有效性

对于手机实名证书，注册时申请者须正确以下信息：

- 个人的真实身份标识信息，包括真实姓名、身份证号码等；
- 手机号码：中国移动 CMCA 通过动态密码或手机服务密码等机制验证手机号码的有效性
- 其他信息，如邮件地址等；

对于移动终端设备证书，注册时申请者须正确以下信息：

- 设备标识信息，如 SIM 卡号等；
- 申请者的信息；

对于终端应用开发者标识证书，注册时申请者须正确以下信息：

- 申请人为机构：按照企业证书信息填写；
- 申请人为个人：按照个人证书信息填写；

终端应用标识证书不需要填写注册信息。

根据《中华人民共和国电子签名法》的规定，申请者未向中国移动CMCA提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、中国移动CMCA造成损失的，承担相应的法律及赔偿责任。

中国移动CMCA注册机构有责任对申请人的身份进行充分的验证，并且要求申请表有验证人签名并注明日期。

4.1.3 证书申请流程

CMCA管理员证书、RA、LRA服务器证书等，证书订户只能向中国移动CMCA中心提交请求并办理业务，不能通过在线方式申请证书。

对于普通用户证书，证书订户可采用现场方式向中国移动CMCA注册中心及受理点提交业务办理请求，同时也可以登陆CMCA官网等自服务网站，在线提交证书申请，除账号证书、终端应用标识证书或不关联实体身份的移动终端设备证书外，其他证书完成在线申请后还需要提供相应纸质、电子证明材料，确保CMCA可以对证书实体的身份进行审核。

对于手机号码、手机实名证书，用户可到中国移动营业网点现场申请，也可以通过短信发送激活口令等方式自助申请；对于手机实名证书，用户需要前往中国移动营业网点现场办理实名身份登记，身份验证通过后，同样可以选择营业网点现场申请和自助申请。

无论现场申请，还是在线申请，CMCA可为证书订户提供渠道创建自助服务用户名和口令，用于订户自行挂失、吊销证书等自助服务。

4.1.3.1 现场申请

对于现场申请，各种证书的申请要求如下：

1) 申请者提交申请资料

- 个人证书，申请者提交一份内容完整的带个人签名的申请表、个人身份证明文件及其复印件一份，如身份证或护照等；
- 对于企业证书，申请者提交一份内容完整的带经办人签名、机构盖章的申请表、加盖公章的组织机构代码证、企业营业执照、经办人的身份证复印件各一份。
- 对于服务器证书，与个人证书或企业证书的申请相同，还需要提供服务器域名、IP 地址或设备标识所有权的证明；
- 对于代码签名证书、终端应用开发者标志证书，与个人证书或企业证书的申请相同。
- 对于手机号码证书，用户在营业网点申请办理，需要验证其手机号码有效性，并在业务受理单签名确认。
- 对于手机实名证书，用户必须在营业网点办理实名登记，提供身份证件及复印件一份，审核通过后在业务受理单签名确认。

2) 注册中心或受理点审核申请资料

3) 审核通过后，注册中心或受理点工作人员为用户提交证书申请

4) CMCA 签发证书

5) 用户接受、使用证书

说明：证书申请表可以从中国移动 CMCA 的网站下载或到中国移动 CMCA 受理点领取。

4.1.3.2 在线证书申请

在线证书申请，在安全性和认证得到保证的情况下，允许申请人通过 Internet、移动网络、短信、STK 或传真提交他们的申请和个人信息。

手机号码、手机实名证书的在线申请方式与其他证书不同，验证手机号码有效性、实名用户身份信息后，用户主要是通过短信激活码、STK 等方式提交证书申请。而其他证书主要是访问自服务网站来提交证书申请。

通常情况下，申请者即使选用在线申请方式，仍须等待中国移动 CMCA 机构或受理点的申请审核，审核方式可包括现场审核、在线审核或其他安全的方式。

特殊情况下，例如已确定身份的客户群体和测试证书的申请流程，申请人提

交在线申请后CMCA不需要审核证书申请。

对于测试证书，中国移动CMCA不承担任何责任。

4.2 证书审核

4.2.1 执行识别与鉴别功能

中国移动CMCA授权的注册机构或受理点对证书申请者提交的信息进行审核。

4.2.2 证书申请批准和拒绝

中国移动CMCA授权的注册机构或受理点根据验证的信息审核通过或拒绝证书申请者的申请。若通过申请，则提交中国移动CMCA。

4.2.3 处理证书申请的时间

在证书申请者提交资料齐全并符合要求的情况下，中国移动CMCA授权的注册机构在3个工作日内完成证书申请的处理，如遇到大规模证书申请批量处理制作等特殊情况，可与客户协商具体处理时限。

4.3 证书签发

包括证书签发过程中电子认证服务机构的各种行为，如电子认证服务机构验证注册机构签名，确认注册机构的权限，并生成证书的过程。

4.3.1 签发证书

证书申请者一旦提交了证书申请，尽管事实上还没有接受证书，但仍被视为该订户已同意发证机构签发其证书。

证书订户采取现场方式到中国移动CMCA授权的注册机构或受理点办理证书申请业务后，中国移动CMCA将为证书申请者生成授权码，并返还给注册机

构或受理点，中国移动 CMCA 授权的注册机构或受理点接收到授权码后，可现场为证书申请者制作证书，证书申请者也可以持授权码自行通过在线的方式下载证书。

如证书订户采取在线方式申请证书，中国移动 CMCA 在审核后会为证书申请者生成授权码，并以安全的方式将授权码发送至订户，订户可以持授权码自行通过在线的方式下载证书。

4.3.2 拒绝签发证书

中国移动 CMCA 授权的注册机构可以根据其独立判断，拒绝给任何人签发证书，并且不对因此而导致的任何损失或费用承担任何责任和义务。

除非证书申请者提交了欺骗性的或伪造的信息，中国移动 CMCA 在拒绝签发证书后，将立即归还证书申请者所付的所有证书购买费用。

4.4 证书接受

4.4.1 证书接受

在中国移动 CMCA 数字证书签发完成后，中国移动 CMCA 授权进行证书业务办理的受理点可现场制作数字证书，并把数字证书及初始密码交给证书申请者；证书申请者也可以在线下载证书。证书申请者从获得证书起就被视为已同意接受证书。

证书申请者接受数字证书后，应妥善保存其证书对应的私钥和口令。

4.4.2 证书申请者的承诺

一旦接受中国移动 CMCA 发证机构签发的证书，从接受之时起直至证书的整个使用有效期内，如果证书申请者不另行通知，那么证书申请者被视为向中国移动 CMCA、注册机构及所有依赖方出如下保证：

1) 客户的每一次数字签名，都是证书申请者自己的数字签名，并且在进行

数字签名时，证书是有效证书并已被证书申请者接受；

2) 未经授权的人员从未访问过证书申请者私钥；
3) 证书申请者向发证机构陈述的所有证书申请相关的信息是真实的；
4) 包含在证书中的信息，都是真实的；
5) 证书将按中国移动 CMCA 电子认证业务规则的规定，只用于经过授权的或其它合法的使用目的；
6) 证书申请者是最终证书申请者而不是发证机构。除非经证书申请者和发证机构间的书面协议明确批准，证书申请者保证不从事发证机构（或类似机构）所从事的功能，例如：把与证书中所含的公钥所对应的私钥用于签发任何证书（或认证其他任何形式的公钥）或证书吊销列表。
7) 一经接受证书，既表示证书申请者知悉和接受中国移动 CMCA 认证业务声明中的所有条款和条件，并知悉和接受相应的证书订户协议。

4.4.3 证书申请者的责任

一经接受证书，证书申请者即同意由下列原因直接或间接造成的任何责任和损失承担法律责任：

1) 证书申请者（或其授权的代理人）虚假地或错误地陈述了事实；
2) 证书申请者未能披露重要事实，而证书申请者的这种有意或无意的错误陈述或失职造成了对发证机构、中国移动 CMCA、或依赖方的欺骗；
3) 证书申请者没有使用可信系统或没有采用必要的合理措施防止其私钥被破译、窃取、泄露、被篡改或被未经授权使用。
4) 证书申请者对中国移动 CMCA 和中国移动 CMCA 授权的 CA 注册机构以及他们的代理商、签约商造成的责任和损失包括：由于上述原因直接或间接造成的责任、损失，任何诉讼、仲裁及一切相关费用，包括但不限于诉讼费用、仲裁费用以及律师费等。对于此处的责任和损失，证书申请者将予以经济赔偿。

4.4.4 证书的发布

一旦证书申请者接受证书，注册机构将在中国移动 CMCA 的信息库或目录服务器及由中国移动 CMCA 和注册机构决定的其它一个或多个信息库里发布证书的副本。证书申请者也可以在其它信息库中公布他们的中国移动 CMCA 证书。

4.5 密钥和证书的使用

4.5.1 订户私钥和证书的使用

订户可以使用私钥进行签名、加密等操作。

订户只能在规定的范围内使用私钥和证书，详见本文 1.4。

订户须妥善保管私钥，避免他人未经授权就使用其私钥和证书。

4.5.2 依赖方公钥和证书的使用

依赖方接收到经数字签名的信息后，应该：

（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） 证书的用途适用于对应的签名

（4） 使用证书上的公钥验证签名

（5） 确认数字签名对应的证书状态正常，没有进入 CRL 列表

依赖方需要采用合适的软硬件进行数字签名的验证工作，当以上任何一个环节失败，依赖方应拒绝接受签名信息。

当依赖方需要发送加密信息给接收方时，须先通过适当的途径获得接收方的加密证书，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收方。

4.5.3 密钥和证书使用的相关责任

- 证书订户和依赖方应严格遵守本 CPS，并承担证书和密钥使用过程中的相关责任。
- 申请者接受到数字证书后，应妥善保存其证书对应的私钥，如因订户个人原因造成密钥的丢失、损坏等，中国移动 CMCA 概不负责。
- 申请者可以从中国移动 CMCA 证书目录服务器中下载个人或其他数字证书。

4.6 证书更新

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

为保证证书及其密钥对的安全有效，中国移动 CMCA 会为签发的证书设置有效期，一般为 1-2 年。证书客户必须在证书有效期到期前，到中国移动 CMCA 授权的注册机构或受理点申请更新证书。更新证书时注册机构根据客户的要求决定新证书是否使用原证书密钥。

4.6.1 证书更新的原因

- 证书有效期即将期满

4.6.2 请求证书更新的实体

由中国移动 CMCA 颁发的原有证书有效期限未到的个人、企业、服务器等提供网上服务和享受网上服务的各种实体，以及其他凡是中国移动 CMCA 各类证书（包括测试证书）的有效期限未到的证书订户。

4.6.3 证书更新流程

中国移动 CMCA 接受现场更新和在线更新这两种方式。更新程序根据中国移动 CMCA 证书的种类不同而不同，但都应遵守证书操作所规定的步骤。

对于CA系统证书（管理员证书、RA、LRA服务器证书等），证书订户只能向中国移动CMCA认证中心提交更新请求，并办理业务，更新流程与证书申请相同。

4.6.3.1 现场更新

现场证书更新流程如下：

1) 申请者到中国移动CMCA授权的注册机构或受理点书面填写“证书更新申请表单”，并注明更新的原因；
2) 中国移动CMCA授权的注册机构对客户提交的证书更新申请进行审核；
   - 对于企业证书、企业服务器证书、企业代码签名证书、终端应用企业开发者标识证书等企业类证书，CMCA注册机构审核机构信息的准确性和有效性、经办人身份信息以及证书申请的授权等，申请表单须经办人签字、机构盖章，如机构证明文件复印件仍在有效期内则不需要重复提交，但需要提交经办人身份证明文件复印件。
   - 对于个人证书、个人服务器证书、个人代码签名、终端应用个人开发者标识证书，CMCA注册机构审核个人信息的准确性和有效性，申请表需个人签名并出示个人身份证件，如身份证复印件在有效期内则不需要重复提交。
   - 对于账号证书，CMCA仅验证其账号有效性
   - 对于手机号码证书，CMCA仅验证其手机号码的有效性
   - 对于手机实名证书，除验证其个人实名身份外，还须验证其手机号码有效性
3) 注册机构审核通过后，提交申请至中国移动CMCA；
4) 注册机构现场为客户更新证书；
5) 新证书签发后，注册机构将证书发给客户，客户接受证书；
6) 新证书签发后旧的证书将被吊销。中国移动CMCA将在1小时内在LDAP上发布客户的新证书。客户旧的证书在24小时内通过CRL发布吊销信息。

4.6.3.2 在线更新

在线证书更新，在安全性和认证得到保证的情况下，允许申请人通过Internet、移动网络、短信、STK或传真提交他们的更新申请以及能验证其身份的证明材料。

通常情况下，申请者即使选用在线更新方式，仍须等待中国移动CMCA机构或受理点的申请审核，审核方式可包括现场审核、在线审核或其他安全的方式。

特殊情况下，例如已确定身份的客户群体和测试证书的更新流程，申请人提交在线更新申请后CMCA不需要审核证书申请。

对于测试证书，中国移动CMCA不承担任何责任。

4.6.4 对更新证书的发布

一旦证书申请者接受了新证书，发证机构将在1小时内在中国移动CMCA的信息库或目录服务器及由中国移动CMCA和注册机构决定的其它一个或多个信息库里发布客户的新证书。客户旧的证书将被吊销，并在24小时内通过CRL发布。

4.7 证书密钥更新

证书密钥更新指订户或其他参与者生成一对新密钥并申请为新公钥签发一个新证书。最终客户的私钥有效期一般均与其证书的有效期一致。

4.7.1 密钥更新的原因

1) 原有证书的密钥泄露。对此，证书持有者负有立即告知中国移动CMCA的义务；
2) 原有证书到期，根据客户要求在更新证书同时，更新其密钥。

4.7.2 请求密钥更新的实体

与证书更新的流程相同，见4.6相关章节。

4.7.3 密钥更新的流程

与证书更新的流程相同，见 4.6 相关章节。

4.7.4 对更新证书的发布

与证书更新的流程相同，见 4.6 相关章节。

4.8 证书变更

证书变更指证书订户的非关键信息变化而签发新证书的情形，而证书的关键信息如个人姓名、单位名称、证件号码等发生变化，证书不能进行变更，而是需要吊销后再申请新的证书。

4.8.1 证书变更的原因

证书变更的主要原因为证书订户的非关键信息信息发生变化：

- 证书客户 Email、地址、联系电话等发生更改
- 其他非关键信息

4.8.2 请求证书变更的实体

与证书更新的流程相同，见 4.6 相关章节。

4.8.3 证书变更的流程

与证书更新的流程相同，见 4.6 相关章节。

证书订户可以通过密码登陆自助服务帐户，自行进行在线信息变更，且证书变更内容为非关键信息，密码验证通过则 CA 中心不需要对此进行审核。

4.8.4 对变更后新证书的发布

与证书更新的流程相同，见 4.6 相关章节。

4.9 证书吊销

4.9.1 证书吊销的原因

以下原因，证书订户可以申请证书吊销：

1) 新的密钥对替代旧的密钥对；
2) 与证书中的公钥相对应的私钥被泄密或客户怀疑自己的密钥失密；
3) 与密钥相关的客户的主题信息改变，证书中的相关信息有所变更；
4) 由于证书不再需要用于原来的用途，而要求中止；
5) 证书的更新费用未收到；
6) 客户不能履行电子认证业务声明或其他协议、法律及法规所规定的责任和义务；
7) 客户申请初始注册时，提供的材料或信息不真实；
8) 证书已被盗用、冒用、伪造或者篡改；
9) CA 机构因运营问题，导致 CA 内部重要数据或 CA 根密钥失密等原因；
10) 其他情况。这些情况可以是因法律或政策的要求中国移动 CMCA 采取的临时吊销措施，也可以是客户申请吊销证书时填写的其他原因。

此外，中国移动 CMCA 授权的注册机构管理员可以对客户证书进行强制吊销，吊销后必须立即通知该证书客户。强制吊销的命令来自于中国移动 CMCA 或中国移动 CMCA 授权的注册机构。

4.9.2 请求证书吊销的实体

由中国移动 CMCA 颁发的原有证书有效期限未到的个人、企业、服务器等提供网上服务和享受网上服务的各种实体，以及其他凡是中国移动 CMCA 各类证书的有效期限未到的证书订户。

中国移动 CMCA 或其授权注册机构也可请求证书吊销。

4.9.3 吊销请求的流程

证书吊销操作可由证书订户自行进行，也可由证书订户或依赖方向中国移动CMCA或授权的注册机构发起请求，由中国移动CMCA或授权的注册机构进行吊销。

证书订户自行吊销证书时，须以自助服务用户名/口令登录中国移动CMCA网站进行操作。

由CMCA或其授权的注册机构吊销证书时，须按照如下流程进行：

- 申请者到中国移动CMCA授权的注册机构或受理点书面填写“证书吊销申请表”，并注明吊销的原因。如果申请人是RA 或LRA，由RA 或LRA填写表单。如果申请人是终端客户，则由终端客户填写表单；
- 中国移动CMCA授权的注册机构按照第三章的要求对客户提交的证书吊销申请进行审核；
- 中国移动CMCA吊销客户证书后，发证机构将通知客户证书被吊销；
- 吊销的客户证书在24 小时内进入CRL 或被直接签发CRL，向外界公布。

中国移动CMCA或其授权的注册机构，在发现证书订户身份资料有问题或其对证书有非法使用情况下，可根据CA策略对终端客户的证书执行吊销操作。

4.9.4 吊销请求宽限期

RA强制吊销可以给予24小时的宽限期。终端客户申请吊销时，RA应在收到吊销请求1小时内吊销证书，没有宽限期。

4.9.5 电子认证服务机构处理吊销请求的时限

中国移动CMCA在收到吊销请求后应立即处理并在1小时内完成。

4.9.6 依赖方检查证书吊销的要求

依赖方应经常检查CRL，包括：

- 在认证各方的使用数字证书前，根据中国移动 CMCA 最新公布的 CRL 检查该证书的状态；
- 验证 CRL 的可靠性和完整性，确保它是经中国移动 CMCA 发行并数字签名的。

依赖方应根据中国移动 CMCA 公布的最新 CRL 确认使用的证书是否被吊销。如果黑名单公布证书已经吊销，而依赖方没有查黑名单，由此造成的损失由依赖方自行承担。

4.9.7 CRL 发布频率

中国移动 CMCA 将通过证书黑名单库 CRL 在 24 小时内公布被吊销的证书，特殊紧急情况下可以立即生效。

对于测试证书的吊销，不提供黑名单公布服务。

4.9.8 在线状态查询要求

能够提供在线状态查询，可通过 OCSP 服务进行证书状态的实时查询。

4.9.9 证书吊销的注意事项

- 中国移动 CMCA 没有公开数字证书吊销原因的业务；
- 证书更新、证书修改、密钥更新后原有证书将被吊销；
- 提交请求时需要指明吊销原因，只有吊销原因是“证书挂起”的证书将来才有可能通过“恢复证书”来被恢复使用；

注意：此处的证书吊销是永久性吊销，不可以进行证书解挂。

4.9.10CA 证书吊销列表的发布周期

CMCA 每年发布一次 CA 证书吊销列表（ARL），当对某个运营 CA 证书做吊销操作后，即时发布 ARL。

4.10 证书挂起

4.10.1证书挂起的原因

- 证书订户暂停使用证书；
- 证书订户的私钥丢失等原因导致证书安全性收到威胁

说明：证书挂起也可以称为证书冻结。

4.10.2请求证书挂起的实体

由中国移动 CMCA 颁发的原有证书有效期限未到的个人、企业、服务器等提供网上服务和享受网上服务的各种实体，以及其他凡是中国移动 CMCA 各类证书的有效期限未到的证书订户。

中国移动 CMCA 或其授权注册机构也可请求证书挂起。

4.10.3挂起请求的流程

普通个人、企业用户可通过 CMCA 官方网站自助服务渠道申请挂失，输入自服务用户名和密码，验证通过后挂失请求成功提交；也可以通过客服电话、现场办理的方式申请人工挂失，CMCA 需要用户提交纸质证明文件以确认身份，验证通过后，CMCA 注册机构业务人员提交挂起请求。

手机用户可通过中国移动电话客服渠道、网上自助渠道等方式申请挂失，输入手机服务密码、动态密码等验证身份，验证通过后挂失请求成功提交。

CMCA 收到挂起请求并验证审核完成后立即完成证书挂起。

客户证书被挂起后，客户必须在证书有效期到期前恢复证书，否则中国移动 CMCA 或中国移动 CMCA 授权的注册机构有权自行注销证书。对此造成的任何后果，中国移动 CMCA 不负任何责任。

4.10.4挂起的期限限制

证书挂起的最长期限为 3 个月，若证书订户在此期限内未能恢复证书，中国

移动 CMCA 或中国移动 CMCA 授权的注册机构将提醒证书订户恢复证书，如确定不再使用，CMCA 有权吊销证书。

4.11 证书解挂

4.11.1证书解挂的原因

证书解挂的原因是证书被挂起，证书解挂仅针对挂起的证书。

说明：证书解挂也可以称为证书解冻。

4.11.2请求证书解挂的实体

由中国移动 CMCA 颁发的原有证书有效期限未到的个人、企业、服务器等提供网上服务和享受网上服务的各种实体，以及其他凡是中国移动 CMCA 各类证书的有效期限未到的证书订户。

中国移动 CMCA 或其授权注册机构也可请求证书解挂。

4.11.3证书解挂的流程

普通个人、企业用户可通过 CMCA 官方网站自助服务渠道申请解挂，输入自服务用户名和密码，验证通过后解挂请求成功提交；也可以通过客服电话、现场办理的方式申请人工解挂，CMCA 需要用户提交纸质证明文件以确认身份，验证通过后，CMCA 注册机构业务人员提交解挂请求。

手机用户可通过中国移动电话客服渠道、网上自助渠道等方式申请解挂，输入手机服务密码、动态密码等验证身份，验证通过后解挂请求成功提交。

CMCA 收到解挂请求并验证审核完成后立即完成证书解挂。

4.12 密钥恢复

4.12.1密钥恢复的原因

- 加密密钥丢失；
- 加密密钥损坏；
- 其他。

4.12.2请求密钥恢复的实体

由中国移动 CMCA 颁发的原有证书有效期限未到的个人、企业、服务器等提供网上服务和享受网上服务的各种实体，以及其他凡是中国移动 CMCA 各类证书的有效期限未到的证书订户。

4.12.3密钥恢复的流程

- 申请者书面填写“密钥恢复申请表单”，并注明恢复的原因。如果申请人是 RA 或 LRA，由 RA 或 LRA 填写表单。如果申请人是终端客户，则由终端客户填写表单；
- 中国移动 CMCA 授权的注册机构按照第三章识别与鉴定对订户提交的密钥恢复申请进行审核；
- 审核通过后，提交申请至中国移动 CMCA
- 发证机构为客户恢复密钥，并提交给订户；

4.12.4密钥恢复的注意事项

- 密钥恢复只能恢复客户的加密密钥；
- 当证书客户接受证书后，应妥善保管签名证书，为其备份；
- 由客户丢失签名证书而造成的后果，中国移动 CMCA 概不负责；

4.13 证书状态服务

中国移动 CMCA 提供两种证书状态服务方式，CRL 发布和 OCSP（在线证书状态查询）服务。

4.13.1CRL

CRL 通过 LDAP 服务器进行发布，其可信度及安全性由 CRL 签发者证书的签名来保证。

客户需要将 CRL 下载到本地后进行验证，包括 CRL 的合法性验证和检查 CRL 中是否包含待检验证书的序列号。

4.13.2OCSP

中国移动 CMCA 提供 OCSP（在线证书状态查询）服务。

4.14 CA 服务终止

CA 服务终止是指证书订户终止与中国移动 CMCA 的服务，包含以下情况：

1) 当证书到期时，证书订户不再延长证书使用期或者不再重新申请证书时，证书订户可以提出服务终止。
2) 在证书的有效期内，由于证书订户的原因而单方面要求终止证书服务。
3) 中国移动 CMCA 将根据证书订户的要求吊销证书。证书订户与中国移动 CMCA 的服务终止。

4.15 密钥生成、备份与恢复

4.15.1加密密钥生成、备份与恢复

证书客户的加密密钥在证书客户申请证书时，由中国移动 CMCA 的 KMC 管理中心生成，并进行托管备份，当证书客户需要恢复加密密钥时，由中国移动

CMCA 中心通过 KMC 为客户取得相应的加密密钥。加密密钥被加密存放在 KMC 管理中心。

4.15.2注意事项

为保证订户签名私钥的安全性，中国移动 CMCA 不保管签名私钥。因此，要求客户妥善保管、备份签名私钥。由于签名私钥遗失所造成的损失由证书客户自己承担。中国移动 CMCA 概不负责。

5. 认证机构设施、管理和操作安全控制

描述物理环境、操作过程和人员的安全控制。中国移动 CMCA 使用这些控制手段来安全地实现密钥生成、实体鉴别、证书签发、证书吊销、审计和归档等功能。并对信息库、注册机构、订户或其他参与者的非技术安全控制进行了描述。

5.1 物理安全控制

5.1.1 物理场地安全

5.1.1.1 物理场地基本情况

中国移动 CMCA 主机房位于湖南省长沙市四方坪湖南移动通信工程公司二楼，机房除了满足基础标准和建筑物标准外，针对 CA 运营的实际风险，证书认证中心划分为 4 个安全区域，共 5 个物理安全层次。4 个安全区域由外到内包括：公共区、服务区、管理区和核心区。5 个物理安全层次由外到内包括：一层为入口、二层为办公区、三层为 CA 服务区与 CA\KM 操作区、四层为 CA 核心区、五层为 KM 核心区。所有机房的建设和管理严格按照中国移动 CMCA 的规定要求，采用高安全性的监控技术，包括视频实时监测、指纹、身份识别卡等监控技术，以确保物理通道的安全。机房内部一律禁止参观，只有经过中国移动 CMCA 授权的人员才能进入授权的部门和工作地点。

5.1.1.2 监控记录

监控记录文件包括对中国移动 CMCA 中心通道上的所有踪迹的记录。中国移动 CMCA 的员工经授权后，两人以上才能进入 4 层以内的区域。对于要进入的来访者，要经中国移动 CMCA 批准后，由一位经中国移动 CMCA 授权的员工陪同。

5.1.1.3 受理点网络系统保护

所有中国移动 CMCA 受理点的网络系统也必须受到保护，确保只有经授权的员工才能进入受理点的系统。中国移动 CMCA 的管理员负责设置和检查受理点管理员的权限。受理点操作员的权限和责任在受理点协议中已作出了规定。

5.1.1.4 根证书的安全

中国移动 CMCA 保证根证书的安全，根证书对应的私钥受到严格的保护。

5.1.2 物理访问

5.1.2.1 防止物理非法进入

中国移动 CMCA 在任何时间，通过身份识别卡和指纹鉴别结合的门禁系统，保证了中国移动 CMCA 中心的物理安全，并防止了物理非法进入。

5.1.2.2 防止未经授权的物理访问

在正常营业时间，未经过授权的人或仅被授权访问有限物理区域的人员不得访问 CA 设施内的受到限制的领域，同防止物理非法进入一样，不仅仅在正常营业时间，而且任何时候，都必须防止未经过授权的物理访问。

5.1.3 电力与空调

- 为了确保计算机设备安全可靠连续运行，本工程引入三路电源，两路由大楼总配电室 UPS 接至屏蔽机房配电柜再分别供给各计算机设备，门禁监控等使用；一路市电工机房照明和专用空调使用。全部电气系统均为三相五线制。本工程所装配的动力配电柜采用常州正泰 XL-21 产品。大量的动力布线按安装规范均穿金属管槽保护。安全可靠，经检验整个系统运行正常。
- 机房采用两台机房专用空调机，活动地板下送风，顶部侧回风，温度控制范围在 18℃~28℃，湿度控制范围在 30%~75%RH，能够满足机房高

热湿比、长时间运行、高可靠性、安全性的要求。经检测达到设计要求。

5.1.4 水患防治

中国移动 CMCA 在机房建设时已采取相应措施，防止水侵蚀，充分保障系统安全。

5.1.5 火灾防护

中国移动 CMCA 通过与专业防火部门协调，实施消防灭火等应急响应措施，避免火灾的威胁，充分保障系统安全。敏感区（三层）、安全区域（四、五层），其建筑物的耐火等级按照 GBJ45《高层民用建筑设计防火规范》中规定的二级耐火等级。

5.1.6 介质存储

介质是指光盘、硬盘、软盘、U 盘、存储卡、磁带等存储介质，存储介质必须得到安全可靠的保护，避免诸如温度、湿度和磁力等环境变化可能产生的危害和破坏。

5.1.7 废物处理

当 CA 机构保存的相关数据已不再需要或存档的期限已满时，中国移动 CMCA 将完全销毁这些数据。所有处理行为将记录在案，以供审查的需要，销毁行为遵守我国的法律。

5.1.8 异地备份

中国移动 CMCA 将提供异地的备份，存储中国移动 CMCA 系统的备份数据和介质，异地备份介质安全要求应符合中国移动 CMCA 备份标准和程序。

本策略确定的备份指对 CA 系统的备份，包括各级 CA 及目录服务、系统配置文件、中国移动 CMCA 网站、加密机、RA 等，当整个 CA 系统出现灾难时，

可以通过异地备份中心的备份数据恢复 CA 系统。

为了保证数据库备份数据的安全，选用磁带等作为备份介质，备份不与现有的数据库在同一物理设备上，避免系统崩溃或磁盘损坏时造成恢复的不可能性。在任何时候，备份都可以把数据库恢复到备份的状态。

对于经常变化的动态数据，每天做备份；对于不常变化的静态或准静态数据，每星期或每月进行一次备份。

5.2 流程安全控制

5.2.1 可信角色

中国移动 CMCA 明确规定了以下关键职能职位为可信角色：

1) 鉴证人员；
2) 证书签发人员；
3) 密钥管理人员；
4) 档案管理人员
5) 秘密分割的分享者
6) 安全管理人员
7) 核心区域维护人员（包括加密设备操作人员）
8) 运营管理人员（包括核心主管、运营服务经理等）
9) 核心技术人员（技术主管、核心研发人员）
10) 主管 CMCA 财务负责人
11) 主管 CMCA 人力资源负责人
12) 核心审计人员

5.2.2 每项任务需要的人数

中国移动 CMCA 确保单个人不能接触、导出、恢复、更新、吊销中国移动 CMCA 的 CA 系统存储的根证书对应的私钥。

至少两个人才能使用一项对参加操作人员保密的密钥分割和合成技术来进行任何密钥恢复的操作。

中国移动 CMCA 对与运行和操作相关的职能有明确的分工，贯彻互相牵制的安全机制。

5.2.3 安全令牌控制

所有中国移动 CMCA 的在职人员的识别与鉴别都是通过各种安全令牌标示的，所有人员必须通过认证后，根据作业性质和职位权限的需要，发放系统操作卡、门禁卡、登录密码、操作证书、作业帐号等安全令牌。对于使用安全令牌的员工，中国移动 CMCA 系统将独立完整地记录其所有的操作行为。

所有中国移动 CMCA 在职人员必须确保：

- 发放的安全令牌只直接属于个人或组织所有
- 发放的安全令牌不允许共享

中国移动 CMCA 的系统和程序通过识别不同的令牌，对操作者进行权限控制。

5.2.4 职责分割原则

中国移动 CMCA 的运营员工和负责 CA 中心系统设计、开发、维护的员工承担不同的职责，双方的岗位互相分离。此外，证书发放关键环节中，信息录入与审核签发人员应由不同的人员担任。

当 CA 中心员工被怀疑，或者已进行了未授权的操作，例如未经授权滥用权利或超出权限使用 CA 中心系统或进行越权操作，CA 中心在得到信息后立即中止该员工进入 CA 中心证书服务体系。根据情节严重程度，实施包括提交司法机关处理等措施。

一旦发现上述情况，CA 中心立即作废或终止该人员的工作。

5.3 人员控制

5.3.1 资格、经历和无过失要求

人事管理制度用以CA中心确定其人员和岗位设置，保障CA中心的安全运营。人事管理制度包括人员的可信度审查、岗位设置等。

中国移动CMCA对员工在资格、经历方面有着严格的要求，而且所聘任的员工要求没有法律方面的过失，具备高可信度。

CA中心应制定可信人员策略并据此进行人员的可信度审查和聘用。可信人员必须接受并通过广泛的背景调查，才能证明他们有能力进行那些关键操作所必须的信任级别。

CA中心对人员的教育水平、从业经历、信用情况等方面进行调查，来评估人员的可信度。进行可信人员背景调查必须遵循国家的有关法律、法规和政策。

5.3.2 背景审查程序

CA中心员工的录取经过严格的审查， 根据岗位需要增加相应可信任的员工。 员工需要有2个月的考察期，根据考察的结果安排相应的工作或者辞退并且剥离岗位。CA中心根据需要对员工进行职责、岗位、技术、政策、法律、安全等方面的培训。

CA中心会对其关键的CA职员进行严格的背景调查。受理点操作员的审查可以参照CA中心对可信任员工的考察方式。 受理点责任单位可以在此基础上，增加考察和培训条款， 但不得违背CA中心证书受理的规程和CA中心证书业务声明。

CA中心确立流程管理规则，据此CA员工受到合同和章程的约束，不许泄露CA中心证书服务体系的敏感信息。所有的员工与CA中心签定保密协议。

5.3.3 培训要求

CA中心对CA中心员工进行以下内容的综合性培训：

- ✧ 公司统一新员工培训
- ✧ CA 中心技术系统介绍
- ✧ CA 中心运营体系介绍
- ✧ 岗位职责及业务流程
- ✧ 相关法律、管理办法等

5.3.4 再培训周期和要求

根据行业法律法规、CA 中心策略调整、系统更新等情况，CA 中心可能要求员工进行继续培训，以适应新的变化。

5.3.5 岗位分离和轮换

CA 中心运营服务员工和负责 CA 中心开发、维护的员工承担不同的职责，双方的岗位互相分离，即开发员工和运营员工分离的原则。

5.3.6 未授权行为的处罚

当 CA 中心员工被怀疑，或者已进行了未授权的操作，例如未经授权滥用权利或超出权限使用 CA 中心系统或进行越权操作，CA 中心在得到信息后立即中止该员工进入 CA 中心证书服务体系。根据情节严重程度，实施包括提交司法机关处理等措施。一旦发现上述情况，CA 中心立即作废或终止该人员的工作。

5.3.7 提供给员工的文档

文档包括《中国移动 CMCA 认证业务规则》、《中国移动 CMCA 运营管理规范》、《中国移动 CMCA 鉴证管理规范》、《中国移动 CMCA 服务管理规范》、相关法律、政策、制度说明以及相关管理制度等。

5.4 安全审计

5.4.1 记录事件的类型

中国移动数字认证中心对如下事件进行记录：

- CA 密钥生命周期内的管理事件，包括，
  - 密钥生成，备份，存储，恢复，归档和销毁。
  - 密码设备生命周期的管理事件，例如接收、使用、卸载和弃用。

  这些记录是密钥管理员完成的电子记录或纸质记录。

- CA 和订户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。
  - 成功或失败的证书操作。

  这些记录由认证系统自动记录，保存在数据库。

- 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。
  - 防火墙和路由器记录的安全事件。

  这些记录由操作系统自动完成，系统维护人员会定期检查系统日志。

- 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。

  这些记录由操作系统自动完成，系统维护人员会定期检查系统日志。

- 中国移动CMCA物理设施的访问记录，如，
  - 授权人员进出。
  - 非授权人员进出及陪同人。
  - 安全存储设施（离线密钥）的访问。

授权人员进出物理设施由物理场地的访问控制系统自动记录。非授权人员进出由陪同人员作纸质记录。

- 可信人员管理记录，包括且不限于，
  - 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

- 日志记录包括如下信息：
  - 每个日志记录的日期和时间。
  - 对于自动日志记录，登记的序列号或序号。
  - 做日志记录的实体的身份。

5.4.2 处理日志的周期

中国移动CMCA每周对记录进行审查，对审查记录行为备案。

5.4.3 审计日志的保存期限

中国移动CMCA在数据库保存审查记录至少三个月，离线存档至少五年。

5.4.4 审计日志的保护

中国移动CMCA执行严格的访问控制管理，确保只有中国移动CMCA授权的人员才能接近这些审查记录。这些记录处于严格的保护状态，严格禁止访问、阅读、修改和删除等操作。

5.4.5 审计日志备份程序

中国移动 CMCA 保证所有的审查记录和审查总结都按照中国移动 CMCA 备份标准和程序进行。根据记录的性质和要求，采用在线和离线的各种备份工具，有实时、每天、每周、每月和每年等各种形式的备份。

5.4.6 审计收集系统

中国移动 CMCA 审计收集系统涉及：

- 证书管理系统；
- 证书签发系统；
- 证书目录系统；
- 远程通信系统；
- 证书审批受理系统；
- 访问控制系统（包括防火墙）；
- 网站、数据库安全保障系统；
- 其他中国移动 CMCA 认为有必要审查的系统。

中国移动 CMCA 全天候准备上述系统的检查管理和审查工具。在需要的时候，中国移动 CMCA 会随时应用这些工具来满足各项审查的要求。

5.4.7 对导致事件实体的处理

中国移动 CMCA 对审查中发现的攻击现象将做详细记录，在法律许可的范围内追溯攻击者，并保留采取相应对策措施的权利，如：切断对攻击者已经开放的服务、递交司法部门处理等措施。

5.4.8 脆弱性评估

对在审查过程中发现的系统的脆弱性，中国移动 CMCA 的相关关键人员，包括审计管理员、安全管理员、系统超级管理员等，或者聘请专业的系统安全评估单位，共同进行相应的脆弱性评估，出具评估报告，并在 1 个月内对系统脆弱

性进行修补。

对在审查过程中发现的物理安全、制度安全、人员安全等方面问题，要及时进行相应的处理和解决。

5.5 记录归档

5.5.1 归档记录的类型

中国移动 CMCA 会对 CA 的数据库定期存档，间隔时间由中国移动 CMCA 自行决定，存档的内容包括中国移动 CMCA 发行的证书和 CRL、审查数据记录、证书申请审批资料等。（签名私钥由实体本身保存，有关私钥的责任由实体本身承担）。

5.5.2 归档记录的保存期限

中国移动 CMCA 中的存档期限一般规定为证书失效后五年。

5.5.3 归档文件的保护

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接近它们。

中国移动 CMCA 保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力的破坏。

中国移动 CMCA 每年会验证存档信息的完整性。

5.5.4 归档文件的备份

所有存档文件的数据库除了保存在中国移动 CMCA 的主要存储库，还将在异地保存其备份。

存档的数据库采取物理或逻辑隔离的方式，与外界不发生信息交互。

只有授权的工作人员才能在监督的情况下，对档案进行读取操作。

中国移动 CMCA 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

所有存档内容都要加时间标识。

5.5.6 归档收集系统

中国移动 CMCA 中的档案收集系统由人工操作和自动操作两部分组成。

5.6 密钥更替

5.6.1 密钥更替定义

在这里密钥更替是指当中国移动 CMCA 根证书到期而需要更换根密钥对时所采取的措施。中国移动 CMCA 根密钥对由加密机产生。证书到期更换密钥时将签发 3 张证书。

- 使用旧的私钥对新的公钥及信息签名生成证书；
- 使用新的私钥对旧的公钥及信息签名生成证书；
- 使用新的私钥对新的公钥及信息签名生成证书。

通过以上 3 张证书达到密钥更换的目的，使新旧证书之间互相认证、信任。

5.6.2 根证书有效期

中国移动 CMCA 根证书有效期为 10 年。在中国移动 CMCA 证书到期之前，中国移动 CMCA 将对根私钥进行更换。密钥转换程序在旧密钥对向新密钥对的转换起着过渡的作用。中国移动 CMCA 密钥转换采用以下方式：

- 一个上级 CA 将在其私钥到期时间小于下级 CA 的生命期之前停止签发新的下级 CA 证书（“停止签发日期”）。
- 产生新的密钥对，签发新的上级 CA 证书。

- 在“停止签发证书的日期”之后，对于批准的下级 CA 或最终客户证书请求，将采用新的 CA 密钥签发证书。

5.6.3 CRL

新的中国移动 CMCA 将继续使用旧的 CA 私钥签发的 CRL，直到由旧的 CA 私钥签发的证书到期为止。

5.7 损害与灾难恢复

CA 系统的灾难恢复，指的是为保证在发生灾害（水灾、风灾、地震等自然灾害，或电力中断、火灾、爆炸等结构型破坏以及人为失误、网络黑客攻击、病毒等操作问题）或战争等攻击而导致 CA 彻底损毁时，能够恢复 CA 的密钥和客户资料。

通过在异地设立灾难备份中心可以实现灾难恢复，灾难备份中心存放了备份的私钥和客户数据。中国移动 CMCA 定期将系统备份服务器中的数据通过磁带备份，以人工方式送到异地容灾备份中心。

当公钥基础设施（PKI）发生灾难性故障时，中国移动 CMCA 拥有恢复运营的能力。首先是确定灾难恢复的重要性以及恢复 PKI 运行的可接受时间。它们是确定 PKI 是否需要一个全面冗余灾难恢复站点的关键因素。

灾难恢复的具体工作包括：

- 制定灾难恢复计划；
- 数据的备份和存储；
- 辅助设备准备；
- 启动灾难恢复计划；
- 灾难恢复所需时间评估。

灾难恢复计划实施：

1. 所有的口令经安全部门主管以及相关的安全管理员、政策审批部门变更。
2. 根据灾难的性质，部分或全部证书需要吊销或以后重新认证。
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，一旦目录管理员从备份中恢复了目录，安全部门和政策审批部门、授权运营部门可从中国移动 CMCA 系统的目录服务器恢复中国移动 CMCA 数据。

5.7.1 事故和损害处理程序

流程为：

1. 保证现有的对外提供的所有设备能够正常提供服务，并且针对每个环节设置紧急预案。
2. 所有的 CA 应用服务都具备基本的监控。
3. 出现故障时，应以尽快正常对外提供服务为目标，记录故障现场，对于影响面大的故障，发现问题 5 分钟内不能快速解决问题的，应考虑启动紧急预案。
4. 严重影响对外服务的故障，应该及时上报主管领导。

5.7.2 计算资源、软件和/或数据的损坏

当计算资源、软件和/或数据收到破坏时，进行以下操作：

1. 恢复环境、CA 系统和备份数据并上线；
2. 为客户恢复证书，重新进行认证；
3. 尽快启动原系统。

5.7.3 实体私钥损害处理程序

对于实体证书私钥的损害，中国移动 CMCA 有如下处理要求和程序：

1） 当客户发现实体证书私钥损害时，必须立即停止使用其私钥，并立即访问中国移动 CMCA 或相应的注册机构的证书服务网站吊销其证书，或者立即通过电话、电子邮件的方式通知中国移动 CMCA 或注册机构吊销其证书。中国移动 CMCA 按§ 4.9 发布证书吊销信息。

2） 当中国移动 CMCA 或注册机构发现证书订户的实体证书私钥受到损害时，中国移动 CMCA 或注册机构将立即吊销证书，并通知证书订户，

订户必须立即停止使用其私钥。中国移动 CMCA 按§ 4.9 发布证书吊销信息。

3） 当中国移动 CMCA 的 CA 证书出现私钥损害时，中国移动 CMCA 将立即吊销该 CA 证书并及时通过广达的途径通知依赖方，然后生成新的 CA 密钥对、签发新的 CA 证书。

5.7.4 灾难后的业务连续性能力

灾难发生后中国移动 CMCA 立即从备份系统或异地备份中心恢复系统和数据，系统上线并对客户提供服务，保持业务持续性。

5.8 电子认证服务机构或注册机构的业务终止

5.8.1 CA 终止原因

CA 终止服务的原因可以分为密钥受损原因和非密钥受损原因。

5.8.2 终止通知

当中国移动 CMCA 打算终止经营时，会在终止经营前三个月给中国移动 CMCA 授权的注册机构、受理点和证书订户书面通知，并在终止服务六十日前向国务院信息产业主管部门报告，按照相关法律规定的步骤进行操作。

5.8.3 终止归档

中国移动 CMCA 会按照相关法律的规定来安排好档案和证书的存档工作。

5.8.4 终止措施

在 CA 中止期间，采用以下措施终止业务：

- 起草 CA 终止声明；
- 通知与 CA 相关的实体；

- 关闭从目录服务器；
- 证书注销；
- 处理存档文件记录；
- 停止认证中心的服务；
- 存档主目录服务器；
- 关闭主目录服务器；
- 管理中国移动 CMCA 系统管理员和中国移动 CMCA 安全管理员；
- 处理加密密钥；
- 处理和存储敏感文档；
- 清除 CA 主机硬件。

5.8.5 RA 的终止

根据中国移动 CMCA 与 RA 签订的协议终止 RA 的业务。

6. 认证系统技术安全控制

6.1 密钥对的生成和安装

由于密钥对是安全机制的关键，所以在 CPS 中制定了相应的规定，确保密钥对的产生、传送、安装等具备保密性、完整性和不可否认性。

6.1.1 CA 密钥对的产生

对于中国移动 CMCA 密钥对，中国移动 CMCA 专门的密钥管理员及若干名接受过相关培训的可信雇员在中国移动 CMCA 核心区屏蔽机房内的离线操作区，按照中国移动 CMCA 的密钥管理手册中规定的密钥生成流程进行产生。中国移动 CMCA 密钥生成流程规定了 CA 密钥产生的安全控制要求及参与人员要求。中国移动 CMCA 的密钥对使用符合国家密码主管部门的要求的密码硬件产生。

6.1.2 订户密钥对的生成

- 加密密钥对

加密密钥对是由中华人民共和国国家密码管理局许可的、中国移动 CMCA 数字证书签发系统支持的加密机设备生成的，由中国移动 CMCA 所属的 KMC 控制管理。

- 签名密钥对

签名密钥对由客户端产生，证书申请者可使用国家密码管理局认可的、中国移动 CMCA 数字证书签发系统支持的介质生成签名密钥对。此签名密钥存储在介质中不可导出，保证中国移动 CMCA 无法复制签名密钥对。

中国移动 CMCA 支持多种介质，如 USBkey。中国移动 CMCA 可根据证书申请者要求或自身选择签名密钥对生成介质。

- 服务器等服务器证书的密钥对由客户自己产生，客户应妥善保管。
- 中国移动 CMCA 在技术、流程和管理上保证密钥对产生的安全性。

6.1.3 私钥传送

中国移动 CMCA 各种运营服务器证书的密钥对由中国移动 CMCA 或其注册机构在设备所在地产生，并在本地保存，不存在私钥的传送问题。

证书订户的加密私钥是在 KMC 产生的，该私钥只保存在 KMC。在加密私钥从 KMC 到订户的传递过程中采用订户的签名公钥和国家密码管理局许可的对称密钥算法对加密私钥进行加密，中国移动 CMCA 无法获得，保证了证书客户的密钥安全。

对于中国移动 CMCA 签发的其他最终客户证书，通常的情况下密钥对在订户本地的密码模块（如 USB Key）中产生，私钥由最终客户保存在本地密码模块中，不存在私钥的传送问题。但在订户通过代理点办理证书业务时，代理点会代最终客户在约定的密码硬件中（如 USB Key）产生证书密钥对，且私钥保存在密码硬件中。在这种情形下，代理点在订户现场见证的前提下，通过安全的途径将保存有证书私钥的密码硬件传送到最终客户手中，并确保在传送过程中私钥不会被非授权的使用、被泄露或被损坏。

6.1.4 公钥传送

对于加密证书，中国移动 CMCA 从 KMC 取得客户公钥后为其签发证书，在此过程中也采用国密办许可的对称密钥算法加密，保证传输中数据的安全。

对于签名证书，订户通过 PKCS#10 格式的证书签名请求信息文件包格式，以电子的方式将公钥提交给中国移动 CMCA 认证中心（或通过其注册机构提交），这些请求通过网络传送时使用安全套接层协议（SSL）或其他安全协议。

6.1.5 电子认证服务机构公钥传送

中国移动 CMCA 的根公钥包含在中国移动 CMCA 根证书中。证书订户可以从中国移动 CMCA 的网站上下载中国移动 CMCA 根证书。

6.1.6 密钥的长度

中国移动 CMCA 所使用的密钥对长度为 2048 位。

中国移动订户所使用的密钥长度至少为 1024 位。

6.1.7 公钥参数的生成

公钥参数由国家密码管理局许可的、中国移动 CMCA 数字证书签发系统支持的硬件产生。

6.1.8 密钥用途

在中国移动 CMCA 证书服务体系中的密钥用途和证书类型紧密相关，基线证书密钥用途如下表所示。

		CA 证书	非实名制证书	企业证书	个人证书	服务器证书	代码签名证书
Criticality		非关键	非关键	非关键	非关键	非关键	非关键
0	digitalSignature	\	设置	设置	设置	设置	设置
1	nonRepudiation	\	\	设置	设置	\	\
2	keyEncipherment	\	设置	设置	设置	设置	\
3	dataEncipherment	\	设置	设置	设置	设置	\
4	keyAgreement	\	\	\	\	设置	\
5	KeyCertSign	设置	\	\	\	\	\
6	CRLSign	设置	\	\	\	\	\
7	EncipherOnly	\	\	\	\	\	\
8	DecipherOnly	\	\	\	\	\	\
9	CodeSinging	\	\	\	\	\	设置

扩展证书密钥用途如下表所示：

		CA证书	手机号码证书	手机实名证书	终端设备证书	手机终端企业开发者代码签名证书	手机终端个人开发者代码签名证书	终端应用标识证书
Criticality		非关键	非关键	非关键	非关键	非关键	非关键	非关键
0	digitalSignature	\	设置	设置	设置	设置	设置	设置
1	nonRepudiation	\	\	设置	\	\	\	\
2	keyEncipherment	\	设置	设置	设置	\	\	\
3	dataEncipherment	\	设置	设置	设置	\	\	\
4	keyAgreement	\	\	\	设置	\	\	\
5	KeyCertSign	设置	\	\	\	\	\	\
6	CRLSign	设置	\	\	\	\	\	\
7	EncipherOnly	\	\	\	\	\	\	\
8	DecipherOnly	\	\	\	\	\	\	\
9	CodeSinging	\	\	\	\	\	\	\

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块的标准和控制

中国移动CMCA使用国家密码管理局许可的产品，密码模块的标准符合国家规定的要求。

6.2.2 私钥多人控制

中国移动CMCA采用M选N多人控制策略激活、使用、停止中国移动CMCA的签名密钥。M>=N，M为3，N为2。

6.2.3 私钥托管

KMC 可以根据客户和法律的需要，对加密密钥进行托管。签名私钥从不进行托管，以保证其不可否认性。

6.2.4 私钥备份

证书订户可以备份他们的私钥，以确保这些私钥的安全。

KMC 备份托管的加密私钥，确保加密私钥的安全。

6.2.5 私钥归档

KMC 提供过期的托管私钥的存档服务。

6.2.6 私钥导入、导出密码模块

在中国移动 CMCA 证书服务体系中，使用中国移动 CMCA 的软件可以把加密私钥导入密码模块中。私钥无法从密码模块中导出。必须通过密码验证之后，才可能使用存储在密码模块中的私钥进行加解密操作。

6.2.7 私钥在密码模块的存储

证书订户应妥善保管私钥，例如将将私钥保存在硬件密码模块中。中国移动 CMCA 订户的签名私钥必须保存在硬件密码模块中。

6.2.8 激活私钥

6.2.8.1 最终客户证书私钥

保存在密码模块中的最终客户证书私钥需在客户输入口令（或 PIN 码）或指纹等密钥保护信息（激活数据）后才被激活，才能能够被使用。

6.2.8.2 运营服务器证书私钥

对于中国移动数字认证中心的运营服务器证书私钥的激活同CA私钥的激活；对于中国移动CMCA注册机构的运营服务器证书私钥，需要专门的安全管理人员输入保护口令后才能激活。

6.2.8.3 CA私钥

中国移动数字认证中心的CA私钥存放在硬件密码模块中，并且其激活数据按CPS §6.2.2进行分割。当需要使用CA私钥时（在线或离线），需要中国移动CMCACA私钥3个秘密分管者中的至少2人和密钥管理员同时到场，由2个秘密分管者输入秘密分割（激活数据）后才能激活。

6.2.9 解除私钥激活状态

对于个人证书和企业证书，当应用软件向密码模块发出设备关闭指令，或密码模块被下载（如硬件密码模块从读卡器中取出）、或客户通过密码管理软件从密码设备登出（logout）、或计算机断电时，私钥被解除激活状态，不能再被使用。

对于服务器等服务器证书，当服务程序关闭、系统注销或系统断电后私钥即进入非激活状态。

对于中国移动CMCA及其注册机构的运营服务器证书的私钥，当CA或RA系统向密码模块发出登出（logout）或密码管理软件向密码模块发出关闭（close）指令，或存放私钥的密码模块断电,，私钥进入非激活状态。

对于中国移动CMCA私钥，当CA系统向密码模块发出登出（logout）或密码管理软件向密码模块发出关闭（close）指令，或存放私钥的硬件密码模块断电,，私钥进入非激活状态。

6.2.10 销毁私钥

在CA私钥生命周期结束后，中国移动CMCA将CA私钥继续保存在一个备份硬件密码模块中，并进行归档，其他的CA私钥备份被安全销毁。归档的

CA 私钥在其归档期限结束后，需在多名可信人员参与的情况下安全销毁。CA 私钥的销毁将确保 CA 私钥从硬件密码模块中彻底删除，不留有任何残余信息。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

中国移动 CMCA 对所有的公钥进行归档处理，通过专门的归档软件对公钥进行归档，并加密保存在数据库中，保证了公钥的安全性。

6.3.2 证书操作期和密钥对使用期

中国移动 CMCA 会在客户申请审核鉴定通过，3 个工作日内将证书颁发给客户，密钥对的使用期限与证书有效期相一致，一般为 1-2 年。

对于 CA 证书，密钥对通过证书更新允许的最长使用期限如下：

- 对于 2048 位主 CA 证书，其密钥对的最长允许使用年限是 10 年。
- 对于 1024 位主 CA 证书，其密钥对的最长允许使用年限是 5 年。
- 对于 2048 位运营 CA 证书，其密钥对的最长允许使用年限是 10 年。
- 对于 1024 位运营 CA 证书，其密钥对的最长允许使用年限是 5 年。

6.4 敏感数据

6.4.1 敏感数据的产生

敏感数据包括中国移动 CMCA 提供的口令、被加密的数据等。中国移动 CMCA 提供唯一的不可猜测的口令。这些口令由中国移动 CMCA 根据授权和操作的许可仅发放给授权客户。

6.4.2 敏感数据的保护

中国移动 CMCA 采取加解密机制等多种方式保护敏感数据，以避免未授权

使用。未授权客户企图使用敏感数据达到预定目的时，敏感数据会自动锁定。

6.5 计算机安全控制

6.5.1 计算机安全技术要求

中国移动 CMCA 的数字证书签发系统的数据文件和设备由中国移动 CMCA 系统管理员维护，未经中国移动 CMCA 管理员授权，其它人员不能操作和控制中国移动 CMCA 系统；其它普通客户无系统账号和密码。中国移动 CMCA 系统部署在多级不同厂家的防火墙之内，确保系统网络安全。中国移动 CMCA 系统密码有最小密码长度要求，而且必须符合复杂度要求，中国移动 CMCA 系统管理员定期更改系统密码。

中国移动 CMCA 系统内的计算机均采用了如防火墙、入侵检测、主机服务端口限制、操作系统安全补丁等防范措施，充分保证了计算机的安全可靠。

6.5.2 计算机安全评估

中国移动 CMCA 使用的密码设备是通过国家密码管理局批准生产的密码设备。其他涉及安全的网络设备、主机、系统软件等都通过了国家相关部门的检测，属合格产品。

6.6 系统生命周期控制

6.6.1 系统开发控制

CMCA 的系统由符合国家相关安全标准和具有密码标准资质的可靠开发商开发，其开发过程符合 CMCA 系统管理的各项规定。

6.6.2 安全管理控制

CMCA 已制定了各种安全策略、管理制度与流程对 CA 运营系统进行安全管理。

6.6.3 生命周期的安全控制

CMCA 的证书认证系统在系统设计过程中充分进行了安全性考虑，在开发过程中有严格的流程进行代码安全管理，在开发完成后进行了严格的安全测试，在正式使用前通过了国家有关部门的系统安全性审查。

6.7 网络的安全控制

中国移动 CMCA 有防火墙以及其他访问控制机制保护，其配置只允许已授权的机器访问。并且通过入侵检测、漏洞扫描等机制配合保证系统网络的安全。

只有经过授权的中国移动 CMCA 员工才能够进入中国移动 CMCA 签发系统、中国移动 CMCA 注册系统、中国移动 CMCA 目录服务器、中国移动 CMCA 证书发布系统等设备或系统。所有授权客户必须有合法的安全令牌，并且通过密码验证。

6.8 时间戳

数字时间戳（DTS：Digital Time Stamp）是对时间信息的数字签名，主要用于实现确定在某一时间某个文件确实存在和确定多个文件在时间上的逻辑关系功能。

7. 证书、证书吊销列表和在线证书状态协议

7.1 证书

中国移动 CMCA 签发的证书均符合 X.509 V3 证书格式。证书的具体格式、内容和 OID 定义遵循国家推荐的 X.509C 标准。

7.1.1 版本号

X.509：V3

7.1.2 证书标准项

域	值或值的限制
版本	V3
序列号	每个证书唯一的值
签名算法	用于签证书的算法的名称（见 CPS § 7.1.3）
签发者 DN	签发者的甄别名。
有效期从	基于国际通用时间(UTC)，和北京时间同步，按 RFC 3280 要求编码
有效期到	基于国际通用时间(UTC)，和北京时间同步，按 RFC 3280 要求编码。有效期限的设置符合 CPS § 6.3.2 规定的限制
主体 DN	证书持有者或实体的甄别名。
公钥	根据 RFC 3280 编码，使用 CPS § 7.1.3 中指定的算法，密钥长度满足 CPS § 6.1.5 指定的要求。
签名	生成和编码满足 RFC 3280 的要求。

7.1.3 证书扩展项

包括授权密钥标识符、主题密钥标识符、密钥使用范围、密钥扩展使用、证书策略、基本限制、CRL 发布点等内容。

7.1.3.1 密钥用法（Key Usage）

该扩展项指定证书密钥对的用法，不同证书该扩展项的设置见 CPS§ 6.1.8。这个扩展项的 criticality 域通常设置为 FALSE。

7.1.3.2 证书策略扩展项（Certificate Policies）

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

7.1.3.3 主体备用名（subjectAltName）

扩展项的使用符合 RFC 3280。此扩展项的 criticality 设为 FALSE。

7.1.3.4 基本限制扩展项（BasicConstraints）

中国移动 CMCA 证书的基本限制扩展项中的主体类型被设为 CA。最终客户证书的基本限制扩展项的主体类型设为最终实体 (End-Entity)。这个扩展项的 criticality 域设置为 FALSE。

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

7.1.3.5 扩展的密钥用法（Extended Key Usage）

对基线证书，扩展的密钥用法扩展项设定如下。

		CA证书	非实名制证书	企业证书	个人证书	服务器证书	代码签名证书
Criticality		非关键	非关键	非关键	非关键	非关键	非关键
0	ServerAuth	\	\	\	\	设置	\
1	ClientAuth	\	设置	设置	设置	\	\
2	CodeSigning	\	\	\	\	\	设置
3	EmailProtection	\	设置	\	设置	\	\
4	Microsoft Server Gated Crypto (SGC) OID: 1.3.6.1.4.1.311.10.3.3	\	\	\	\	设置	\
5	Netscape SGC - OID: 2.16.840.1.113730.4.1	\	\	\	\	设置	\

对扩展证书，扩展的密钥用法扩展项设定如下。

		CA证书	手机号码证书	手机实名证书	终端设备证书	手机终端企业开发者代码签名证书	手机终端个人开发者代码签名证书	终端应用标识证书
Criticality		非关键	非关键	非关键	非关键	非关键	非关键	非关键
0	ServerAuth	\	\	\	设置	\	\	\
1	ClientAuth	\	设置	设置	\	\	\	\
2	CodeSigning	\	\	\	\	设置	设置	设置
3	EmailProtection	\	设置	设置	\	\	\	\
4	Microsoft Server Gated Crypto (SGC) OID: 1.3.6.1.4.1.311.10.3.3	\	\	\	设置	\	\	\
5	Netscape SGC - OID: 2.16.840.1.113730.4.1	\	\	\	设置	\	\	\

7.1.3.6 CRL 的分发点（CRL Distribution Points）

中国移动 CMCA 签发的证书中包含 CRL 的分发点扩展项，依赖方可根据该扩展项提供地址和协议下载 CRL。此扩展项的 criticality 项应设为 FALSE。

7.1.3.7 签发 CA 密钥标识符

中国移动 CMCA 最终客户证书及中级 CA 证书中有签发 CA 密钥标识符扩展项，当证书签发者包含主体密钥标识扩展项时，签发 CA 密钥标识符由 160 位的签发证书的 CA 的公钥进行 SHA-1 散列运算后的值构成；否则，它将包含签发 CA 的主体 DN 和序列号。这个扩展项的 criticality 域设置为 FALSE。

7.1.3.8 主体密钥标识符

当证书包含主体密钥标识符扩展项时，该值由证书主体的公钥产生。使用该扩展项时，其扩展项的 criticality 域设为 FALSE。

7.1.4 密钥算法对象标识符

中国移动 CMCA 签发的证书按照 RFC 3280 标准，用 sha1RSA 算法签名：

sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}。

7.1.5 名称格式

采用 X.500 甄别名格式。

7.2 证书吊销列表

中国移动 CMCA 定期签发 CRL（证书废除列表），采用 X.509V2 格式。

7.2.1 版本号

X.509：V2。

7.2.2 CRL 和 CRL 条目扩展项

包含 CRL 颁发者、签名算法等内容，中国移动 CMCA 每隔 24 小时自动发布最新的 CRL。

域	值或值的限制
版本	V2
签名算法	签发 CRL 的算法。使用 sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)算法签名。
颁发者	签发 CRL 的实体。颁发者甄别名。

域	值或值的限制
有效期	CRL 的签发日期。
下次更新	CRL 下次签发的日期。对于 CA，隔 2 年；对于最终客户证书 24 小时。
吊销的证书	列出吊销的证书，包括吊销证书的序列号和吊销日期。

7.3 在线证书状态查询协议

中国移动 CMCA 为证书客户提供 OCSP（在线证书状态查询）服务，OCSP 为 CRL 的有效补充，方便证书订户及时查询证书状态信息。

版本号为 OCSP：V1。

域	值或值的限制
状态	响应状态，包括成功、请求格式错误、内部错误、稍候重试、请求没有签名和请求签名证书无授权，当状态为成功时必须包括以下各项。
版本	V1
签名算法	签发 OCSP 的算法。使用 sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)算法签名。
颁发者	签发 OCSP 的实体。签发者公钥的 SHA1 数据摘要值和证书甄别名。
产生时间	OCSP 响应的产生时间。
证书状态列表	包括请求中所查询的证书状态列表。每个证书状态包括证书标识、证书状态以及证书吊销信息。
证书标识	包括数据摘要算法(SHA1，OID: 1.3.14.3.2.26)、证书甄别名数据摘要值、证书公钥数据摘要值和证书序列号。
证书状态	证书的最新状态，包括有效、吊销和未知。
证书吊销信息	当返回证书状态为吊销时包含吊销时间和吊销原因。

8 认证机构审计和其他评估

8.1 审计的频率或情形

8.1.1 中国移动 CMCA 的审计

中国移动CMCA将定期或不定期对自身运营体系包括中国移动CMCA的关联单位（如中国移动CMCA授权的注册机构、受理点等）的业务流程和运营操作进行内部审计和监督审计，检验其是否符合本CPS和相关规范的规定，审计频率和周期可由中国移动CMCA审计部门决定。

中国移动CMCA还将接受行业主管部门的不定期业务检查与审计，也可以聘请外部审计机构进行审计评估。

8.1.2 中国移动 CMCA 对关联单位的审计

中国移动CMCA对其关联单位实行定期或不定期审计（一般审计周期为1年），特殊情况不超过2次/年。审计人员由中国移动CMCA审计部门指派。审计人员必须熟悉中国移动CMCA的规范和信任服务的相关知识，了解保证安全的基本知识，按照中国移动CMCA的规范、协议、履行责任业务等情况，独立、公正地对关联单位做出合格或不合格的结论。

中国移动CMCA有权根据上级的审计结果和自身的审计结果，取消对下属单位的授权或重新授权。审计结果根据被审计单位的要求而决定是否公布。

中国移动CMCA有权对关联单位的审计收取审计费，审计费用在中国移动CMCA与关联单位的合作协议中体现。

8.2 审计者的资质

对中国移动CMCA实施规范审计的外部审计者所具有的资质和经验必须符合监管法律和行业准则规定的要求，包括：

1) 必须是经许可的、有营业执照的、具有计算机安全专门技术知识的审计

人员或审计评估机构，且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) 熟悉 CA 行业规范与业务，熟悉电子认证服务；

8.3 审计者与中国移动 CMCA 的关系

8.3.1 审计者与中国移动 CMCA 的关系

中国移动 CMCA 可对自身运营体系包括中国移动 CMCA 的关联单位（如中国移动 CMCA 授权的注册审核机构、受理点等）的业务流程和运营操作进行内部审计和监督审计。

8.3.2 审计报告与中国移动 CMCA 的关系

内部审计由中国移动 CMCA 审计小组提供内部审计报告；

外部审计，审计报告的作者是外部审计机构，中国移动 CMCA 对其内容不负任何责任，同时中国移动 CMCA 也不对这些审计报告发表任何观点，也不会对由于信任审计报告中有关中国移动 CMCA 的内容而导致的任何损失负责。

8.4 审计内容

对中国移动 CMCA 规范审计应包括：

1) 中国移动 CMCA 支持的证书认证操作规程是否完全与本认证业务声明表达一致，包括中国移动 CMCA 的技术、手续和员工的相关管理政策和业务声明。

2) 中国移动 CMCA 是否实施了相关技术、管理、相关政策和业务声明。

3) 审计者或中国移动 CMCA 认为有必要审计的其他方面。

8.5 对问题与不足采取的措施

如果在审计过程中发现执行规范有不足之处，中国移动 CMCA 将根据审计报告的内容准备一份整改方案，并尽快落实解决。

8.6 评估结果的传达与发布

除非法律明确要求，中国移动 CMCA 一般不公开审计结果。但对于中国移动 CMCA 的关联单位的监督审计结果，中国移动 CMCA 审计部门将按照中国移动 CMCA 业务审计管理规范的具体规定向其公布。

9 法律责任和其他业务条款

9.1 费用

9.1.1 证书费用

中国移动 CMCA 根据制定的收费策略向证书订户收取相关费用，中国移动 CMCA 可在收费标准的基础上，对不同的行业应用或项目提供相应的资费优惠政策，并通知证书申请者或订户。

9.1.2 退款策略

在证书操作和签发证书的过程中，中国移动 CMCA 遵守并保持严格的操作程序和策略。如果中国移动 CMCA 违背了 CPS 有关订户或订户证书方面所规定的责任或其它重大义务，订户可以要求中国移动 CMCA 吊销证书并退款。在中国移动 CMCA 吊销了订户的证书后，中国移动 CMCA 将立即把订户为该证书所支付的全额费用退还给订户。订户需要填写退款申请表，并发送给中国移动 CMCA，以要求退款。此退款程序不限制订户得到其它的赔偿。

除上述情况外，中国移动 CMCA 不接受订户其他理由的退款申请。

9.2 财务责任

中国移动 CMCA 及其授权的分支机构应该具有维持其运作和履行其责任的经济能力，应该有能力承担对订户、依赖方等造成的风险。

中国移动 CMCA 每年定期委托公正、客观的第三方进行财务审核。

中国移动 CMCA 对于证书运营服务产生的风险，为了保障客户的权益，将建立财务赔偿基金，用来支付由于证书业务产生的赔偿。

9.2.1 保险范围

中国移动 CMCA 根据业务发展情况决定其投保策略，包括但不限于：

1、 建筑物与硬件设施的火灾等意外险；

2、 证书责任险，保险范围涵盖中国移动 CMCA 证书订户和证书依赖方保险时间为在证书的有效期内。

中国移动 CMCA 在保险范围内仅承担有限责任。

9.2.2 对最终实体的保险或担保

中国移动 CMCA 的证书最终实体包括证书订户和证书依赖方，中国移动 CMCA 对其负有保险或担保责任。

9.3 业务信息保密

9.3.1 保密信息范围

1) 中国移动 CMCA 与中国移动 CMCA 授权的发证机关之间、中国移动 CMCA 与依赖方/订户之间、中国移动 CMCA 授权的注册机构与依赖方/订户之间的协议、往来函和商务协定等，除非法律明确规定，一般不能在未经另一方许可的前提下擅自公开。

2) 对中国移动 CMCA 或关联机构的审计报告、审计结果等相关信息是保密信息，除了中国移动 CMCA 授权和信任的员工，不能泄露给其他任何人。这

些信息除了用于审查目的或法律规定的目的外，不能用于其他用途。

3) 有关中国移动 CMCA 机构运作的信息只能在严格指定的情况下，才能传授给中国移动 CMCA 授权的员工。

4) 突发事件的应对计划和灾难事件的恢复计划。

5) 控制发证机关软硬件操作的安全措施和管理证书服务及注册服务的安全措施。

6) 除非法律明文规定，中国移动 CMCA 没有义务公布或透露证书订户证书以外的信息。

7) 证书订户的私钥是机密的，证书订户应妥善保管，不能公布给未经授权的第三方，因证书订户泄漏私钥造成的损失由订户自行承担。

9.3.2 不属于保密的信息

1) 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。

2) 中国移动 CMCA 目录服务器中公布证书的作废信息，供网上查询。

3) 证书、证书内包括的公钥、证书中包括的订户信息，是可以公开的。

9.3.3 对业务信息保密的责任

中国移动 CMCA、订户、依赖方、关联机构以及其他参与者，都有义务按照本 CPS 的规定，承担相应的保护保密信息的责任。

当中国移动 CMCA 在任何法律、法规或规章条款的要求下，或在法院等权力部门要求下必须披露本认证业务声明中具有保密性质的信息时，中国移动 CMCA 可以按照法律、法规或规章条款以及法院的判定的要求，向执法部门公布相关的保密信息。这种披露不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，要求中国移动 CMCA 公开或披露他所拥有的保密信息时，该所有者必须提出书面授权，表示其公开或者披露的申请，中国移动 CMCA 可满足其申请。

如果这种披露保密信息的行为涉及任何其他方的赔偿义务，中国移动 CMCA 不应承担任何与此相关的或由于公开保密信息所造成的损失。保密信息的所有者

应当承担与此相关的或由于公开保密信息引起的所有赔偿责任。

9.4 个人隐私保密

9.4.1 隐私保密方案

客户的个人隐私信息存储于CA、RA数据库中，证书的密钥加密存储于数据库中，未经授权无法取得。

9.4.2 作为隐私处理的信息

在申请证书时提供的私人信息，无论该申请是否被批准，除了订户的基本信息和身份认证资料都被作为隐私处理，非经订户同意或者法律法规及公权力部门的合法要求，不会任意对外公开。

9.4.3 不被视为隐私的信息

证书内包括的信息以及该证书的状态信息等是可以公开的，将不被视为隐私信息。

9.4.4 保护隐私的责任

中国移动CMCA、订户、依赖方、关联机构以及其他参与者，都有义务按照本CPS的规定，承担相应的保护隐私信息的责任。

9.4.5 依法律或行政程序的信息披露

中国移动CMCA在任何法律法规或者法院以及公权力部门通过行政程序的要求下，可以向特定对象公布相关的隐私信息，而且这种披露不能被视为违反来隐私保护义务，如果这种隐私披露导致了任何损失，中国移动CMCA对此不应承担任何责任。

9.4.6 其他信息披露情形

中国移动 CMCA 在信息所有者书面授权的情况下，可以向特定对象公布相关的隐私信息，而且这种披露不能被视为违反来隐私保护义务，如果这种隐私披露导致了任何损失，中国移动 CMCA 对此不应承担任何责任。

9.5 知识产权

中国移动 CMCA 享有并保留除中国移动 CMCA 系统软件之外的知识产权，包括中国移动 CMCA 的名称权、商标权、使用权、利益分享权、商业秘密、相关的文件和使用手册等。

有关机构在征得中国中国移动 CMCA 认证中心的同意后，可以使用相关的文件和手册，并有责任和义务提出修改意见。

在没有中国移动 CMCA 预先书面同意的情况下，使用者不能在任何证书到期、作废、或终止的期间或之后，使用或接受任何中国移动 CMCA 使用的名称、商标、交易形式或可能与之相混淆的名称、商标、交易形式或商务称号。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

9.6.1.1 中国移动 CMCA 的责任和义务

中国移动 CMCA 应承担的唯一和绝对的责任和义务是：

- 保证中国移动 CMCA 机构本身使用和发放的公钥算法在现有通常技术条件下不会被攻破；
- 保证中国移动 CMCA 的签名私钥在中国移动 CMCACSF 内部得到安全的存放和保护；
- 中国移动 CMCA 建立和执行的安全机制符合国家政策的规定。

除上述规定的职责条款，中国移动 CMCA、中国移动 CMCA 的服务机构、

中国移动 CMCA 授权的注册机构、中国移动 CMCA 的雇员不承担其它任何义务。必须指出，本认证业务声明的内容，没有任何信息可以暗示或解释成中国移动 CMCA 必须承担其它的义务或中国移动 CMCA 必须对其行为作出其它的承诺。

9.6.1.2 客观意外和不可抗力

中国移动 CMCA 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损失、损坏或赔偿责任。这些事件包括劳动纠纷、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。

9.6.1.3 其他

在第 9.6.1.2 条款所罗列的任何情况下，中国移动 CMCA 由于受到影响，可免除第 9.6.1.1 条款、本认证业务声明和相应的 CP 规定的责任和义务。

由于技术的进步与发展，为保证证书的安全性，中国移动 CMCA 会要求证书订户及时更换证书以保证中国移动 CMCA 能更好地履行 9.6.1.1 条款。

9.6.2 注册机构的陈述与担保

注册机构必须遵守本认证业务声明的条款，以及《中国移动 CMCA 运营管理规范》和《中国移动 CMCA RA 管理规范》等规范制度，

注册机构均须遵守并按照鉴证规范在证书签发前严格执行鉴证流程，确保证书签发的准确性和可靠性。

9.6.3 订户的陈述与担保

所有的证书订户必须严格遵守关于证书申请以及私钥的所有权和安全保存相关的程序：

- 证书订户在证书申请表上或在线填列的所有声明和信息必须是完整、准确和真实的，可供中国移动 CMCA 或受理点检查和核实；

- 证书订户必须严格遵守和服从认证业务声明规定的或者由中国移动CMCA 推荐使用的安全措施；
- 证书订户需熟悉本认证业务声明的条例和与证书相关的证书政策，还需遵守证书订户证书使用方面的有关限制；
- 一旦发生任何可能导致安全性危机的情况，如证书订户遗失私钥、遗忘或泄密以及其他情况，证书订户应立刻通知中国移动 CMCA 或中国移动 CMCA 授权的注册机构，申请采取挂失、吊销等处理措施。

9.6.4 依赖方的陈述与担保

依赖方在信赖中国移动 CMCA 证书的时候，必须保证遵守和实施以下条款：

- 依赖方熟悉相关的证书政策，了解证书的使用目的。
- 依赖方在信赖任何 CA 证书前，必须查最新的 CRL 以检查证书的状态，只有确认该证书没有被作废时，该证书才有效。
- 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这里的有关条例。

9.6.5 其他参与者的陈述与担保

其他参与者如目录服务提供者、以及其他提供电子认证相关服务的实体需要遵守中国移动 CMCA 的 CPS。

9.7 担保免责

如果证书申请人故意或无意地提供不完整、不可靠或已过期的信息，而他又根据正常的流程提供了必须的审核文件，由此得到了中国移动 CMCA 机构签发的数字证书。由此引起的经济纠纷应由申请人全部承担，中国移动 CMCA 不承担与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帮助。

中国移动 CMCA 不承担任何其他未经授权的人或组织以中国移动 CMCA 名义编撰、发表或散布不可信赖的信息所引起的法律责任。

中国移动 CMCA 在法律许可的范围内，根据受害者或法律的要求如实提供

电子交易和作业中“不可抵赖”的数字签名依据，但并不对此承担法律责任。

中国移动 CMCA 不对任何一方在信赖证书或使用证书过程中引起的直接或间接的损失承担责任。

9.8 有限责任

对于由于中国移动 CMCA 自身原因，如没有严格按业务流程进行证书审批导致证书的错误签发、假冒，或管理上的疏忽导致 CA 私钥泄漏、盗用等，造成了证书订户、依赖方的损失，中国移动 CMCA 将承担相应的赔偿责任，但这种责任是有限的。

中国移动 CMCA 在对外服务过程中只承担对外声明的、本 CPS 中规定的、对外签署的任何协议中所规定的有限责任。中国移动 CMCA 在与客户和依赖方签署的协议中，对于因客户或依赖方的原因造成的损害不具有赔偿义务。

9.9 赔偿

在中国移动 CMCA 违反了规定的职责，中国移动 CMCA 承担赔偿责任（法律免责除外）。

9.9.1 赔偿条件

有下列情形之一的，中国移动CMCA承担有限的赔偿责任：

1） 由于中国移动 CMCA 的未授权使用或泄露造成的客户私钥泄露，中国移动 CMCA 进行赔偿；

2） 当中国移动 CMCA 由于故意违反本 CPS 造成的客户的经济损失，中国移动 CMCA 进行赔偿；

3） 由于中国移动 CMCA 自身原因造成的颁发给客户的证书信息出现实质性错误，中国移动 CMCA 进行赔偿。 中国移动 CMCA 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；

4） 由于中国移动 CMCA 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；

订户有下列情形之一，给中国移动CMCA、依赖方造成损失的，应当承担赔偿责任：

1） 提供的资料或者信息不真实、不完整或者不准确的；

2） 证书中的信息有变更，未终止使用该证书并通知各方的；

3） 订户没有使用可信系统保护私钥，或者没有采取必要的注意防止订户私钥的安全损害、丢失、泄漏、修改或非授权的使用；

4） 知悉证书私钥已经丢失或者可能已经丢失时，未终止使用该证书并通知各方的；

5） 订户使用的名字（包括但不限于通用名、域名和 e-mail 地址）破坏了第三方的知识产权的；

6） 超过证书的有效期限使用证书的；

7） 使用证书用于违法、犯罪活动的。

在如下情况，依赖方对自身原因造成的中国移动CMCA损失承担责任：

1） 依赖方没有执行依赖方职责义务；

2） 依赖方在不合理的环境下信赖一个证书；

3） 而依赖方没有检查证书状态确定证书是否过期或吊销。

有下列情形之一的，中国移动CMCA不承担赔付责任：

1） 因订户原因致使依赖方遭受损失的；

2） 依赖方未经检验证书的状态即决定信赖证书的；

3） 依赖方明知或者应当知道证书存在超范围使用、超期限使用、被人窃取或者信息错误等情况，仍然信赖该证书并从事有关活动的；

4） 因不可抗力原因导致订户或者依赖方遭受损失的。

9.9.2 赔偿限制

根据证书的类别，中国移动CMCA所承担的有限责任的赔偿限额如下：

证书等级	证书类型	赔偿限额
基线证书	非实名制证书	不赔偿

	个人证书	最高人民币20,000元
	企业证书	最高人民币50,000元
	服务器证书	最高人民币50,000元
	代码签名证书	最高人民币50,000元
扩展证书	手机号码证书	最高人民币1,000元
	手机实名证书	最高人民币20,000元
	移动终端设备证书	最高人民币2,000元
	终端应用开发者标识证书	最高人民币20,000元
	终端应用标识证书	最高人民币20,000元

1） 中国移动 CMCA 所有的赔偿义务不得高于这种证书适用的债务上限，这种上限可以由中国移动 CMCA 改动。

2） 中国移动 CMCA 只有在 CA 证书有效期限内承担这种损失或损害赔偿。

3） 中国移动 CMCA 只对由于自身原因造成的客户直接损失承担责任，对间接的损失不承担责任。

9.9.3 其他机构赔偿

注册机构的责任在注册机构和中国移动 CMCA 之间签定的注册机构协议中表明。

9.10 有效期限与终止

中国移动 CMCA 的 CPS 自发布之日起正式生效，CPS 中将详细注明版本号及发布日期，最新版本的 CPS 请访问中国移动 CMCA 网站以获得，对具体个人不做另行通知，当新版本的 CPS 正式发布生效，则旧版本的 CPS 将自动终止。

9.11 修订

中国移动 CMCA 有权在合适的时间修订、修改和改变本认证业务声明中任何术语、条件和条款，而且无须预先通知任何一方。

中国移动 CMCA 有权在中国移动 CMCA 的自主数据库中设置和公布修改结果，或以其他方式（如修改 CPS 版本的形式或在网站上）公布。

所有的修订、修改和改变在公布后立刻生效。证书订户如不在修改结果后公布的限定时间内申请废止证书，就视为同意这种修正、修改和变化。

9.12 争议处理

若本认证业务声明的规定与其他规定、指导方针相互抵触，客户必须接受本认证业务声明的约束。

凡因本认证业务声明引起的或与本认证业务声明有关的一切争议，当事人均同意由卓望数码技术（深圳）有限公司住所地人民法院管辖。

9.13 管辖法律

本认证业务声明在各方面服从中华人民共和国电子签名法的管制和解释。

9.14 适用的法律

无论合同或其他法律条款的选择及无论是否在中国建立商业关系，中国移动 CMCA 认证业务声明的执行、解释、翻译和有效性均适用中华人民共和国的法律。

法律的选择是确保对所有客户有统一的程序和解释，而不管他们在何地居住以及在何处使用证书。

9.15 一般条款

9.15.1 完整协议

本协议和附件构成双方就所涉事项达成的全部理解和同意，并取代所有双方先前达成的暂行协议或谅解备忘录。

9.15.2 转让

无论是各方明示的或暗示的继任者、执行者、继承者、代表、管理者和受让人，中国移动 CMCA 的 CPS 均保证其权益，并对其有约束力。各方可根据法律转让（包括并合或转让可控有价证券）中国移动 CMCA 的 CPS 详述的权利和义务。

9.15.3 分割性

中国移动 CMCA 的 CPS 的任何条款或其应用，如果因为任何原因或在任何范围内发现无效或不能执行，那么 CPS 其余的部分（以及对它方的无效或不能执行的条款的适用）将会作出合理的解释以反映当事人的原意。相关当事人了解并同意，中国移动 CMCA 的 **CPS** 所规定的责任限制、保证或其它免责条款或限制、或损害赔偿的排除等，系可独立于其它条款的个别条款，并可加以执行。

9.15.4 不可抗力

中国移动 CMCA 和发证机构将不对以下超越它们控制能力的事件所造成中国移动 CMCA 的 CPS 规定的担保责任违反、延误或无法履行负责。不可抗力一般包括劳动纠纷、交易一方故意或无意的行为、罢工、暴动、瘟疫、骚动、战争、断电、火灾、爆炸、地震、水灾或其他大灾难等。

9.16 其他条款

中国移动 CMCA 与具体客户协商后另行确定其他条款，包括未在上述说明的其他相关内容条款。