



---

---

# 中国移动 CMCA 全球信任证书业务规则

---

---

**<版本: V0.2>**

**生效日期: 2020 年 10 月 12 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	新建文档	2020.4.10	委员会工作组
V0.1A	修订文档	2020.4.22	委员会工作组
V0.2	修订文档	2020.10.12	委员会工作组

# 目 录

<b>1. 概括性描述</b>	<b>1</b>
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	3
1.3 电子认证活动参与者	3
1.3.1 电子认证服务机构	3
1.3.2 注册机构	3
1.3.3 订户	3
1.3.4 依赖方	4
1.3.5 其他参与者	4
1.4 证书应用	4
1.4.1 适合的证书应用	4
1.4.2 限制/禁止的证书应用	5
1.5 策略管理	5
1.5.1 策略文档管理机构	5
1.5.2 联系人	5
1.5.3 决定 CPS 符合策略的机构	6
1.5.4 CPS 批准程序	6
1.6 定义和缩写	6
<b>2. 信息发布与信息管理</b>	<b>7</b>
2.1 信息库	7
2.1.1 信息库监督、监控机制	7
2.1.2 信息库内部数据维护	8
2.2 信息发布	8
2.2.1 CPS 的发布	8
2.2.2 公众信息的发布	9
2.2.3 认证信息的发布	9
2.3 发布的时间或频率	9
2.4 信息库访问控制	9
<b>3. 身份标识与鉴别</b>	<b>10</b>
3.1 命名	10
3.1.1 名称类型	10
3.1.2 对名称有意义的要求	10
3.1.3 订户的匿名或伪名	10
3.1.4 理解不同名称形式的规则	10
3.1.5 名称的唯一性	11
3.1.6 商标的承认、鉴别和角色	11

3.2 初始身份确认.....	11
3.2.1 证明拥有私钥的方法.....	11
3.2.2 组织机构身份的鉴别.....	11
3.2.3 个人身份的鉴别.....	17
3.2.4 没有验证的订户信息.....	17
3.2.5 授权确认.....	17
3.2.6 互操作准则.....	17
3.3 更新请求的标识与鉴别.....	18
3.3.1 常规更新的标识与鉴别.....	18
3.3.2 吊销后更新的标识与鉴别.....	18
3.4 吊销请求的标识与鉴别.....	19
3.4.1 证书吊销情况.....	19
3.4.2 吊销操作.....	19
4. 证书生命周期操作要求.....	20
4.1 证书申请.....	20
4.1.1 证书申请实体.....	20
4.1.2 注册过程与责任.....	20
4.2 证书审核.....	21
4.2.1 执行识别与鉴别功能.....	21
4.2.2 CMCA 证书申请批准和拒绝.....	22
4.2.3 处理证书申请的时间.....	22
4.3 证书签发.....	22
4.3.1 证书签发中注册机构和电子认证服务机构的行为.....	22
4.3.2 电子认证服务机构和注册机构对订户的通告.....	23
4.4 证书接受.....	23
4.4.1 构成接受证书的行为.....	23
4.4.2 电子认证服务机构对证书的发布.....	24
4.4.3 CMCA 对其他实体的通告.....	24
4.5 密钥和证书的使用.....	24
4.5.1 订户私钥和证书的使用.....	24
4.5.2 依赖方公钥和证书的使用.....	25
4.6 证书更新.....	25
4.6.1 证书更新的原因.....	25
4.6.2 请求证书更新的实体.....	25
4.6.3 证书更新流程.....	25
4.6.4 颁发新证书时对订户的通告.....	25
4.6.5 构成接受更新证书的行为.....	26
4.6.6 电子认证服务机构对更新证书的发布.....	26
4.6.7 电子认证服务机构对其他实体的通告.....	26
4.7 证书密钥更新.....	26
4.7.1 证书密钥更新的情形.....	26
4.7.2 请求证书密钥更新的实体.....	26

4.7.3 证书密钥更新请求的处理.....	26
4.7.4 颁发新证书时对订户的通告.....	26
4.7.5 构成接受密钥更新证书的行为.....	27
4.7.6 电子认证服务机构对密钥更新证书的发布.....	27
4.7.7 电子认证服务机构对其他实体的通告.....	27
4.8 证书变更.....	27
4.8.1 证书变更的原因.....	27
4.8.2 请求证书变更的实体.....	27
4.8.3 证书变更的流程.....	27
4.8.4 颁发新证书时对订户的通告.....	28
4.8.5 构成接受变更证书的行为.....	28
4.8.6 电子认证服务机构对变更证书的发布.....	28
4.8.7 电子认证服务机构对其他实体的通告.....	28
4.9 证书吊销和挂起.....	28
4.9.1 证书吊销的情形.....	28
4.9.2 请求证书吊销的实体.....	30
4.9.3 吊销请求的流程.....	30
4.9.4 吊销请求宽限期.....	32
4.9.5 电子认证服务机构处理吊销请求的时限.....	32
4.9.6 依赖方检查证书吊销的要求.....	33
4.9.7 CRL 发布频率.....	33
4.9.8 CRL 发布的最大滞后时间.....	33
4.9.9 在线状态查询的可用性.....	33
4.9.10 在线状态查询要求.....	34
4.9.11 吊销信息的其他发布形式.....	35
4.9.12 密钥损害的特别要求.....	35
4.9.13 证书挂起的情形.....	35
4.9.14 请求证书挂起的实体.....	35
4.9.15 挂起请求的流程.....	35
4.9.16 挂起的期限限制.....	35
4.10 证书状态服务.....	36
4.10.1 操作特性.....	36
4.10.2 服务可用性.....	36
4.10.3 可选特征.....	36
4.11 订购结束.....	36
4.12 密钥托管与恢复.....	36
4.12.1 密钥恢复的策略与行为.....	36
4.12.2 会话密钥的封装与恢复的策略与行为.....	37
<b>5. 认证机构设施、管理和操作安全控制.....</b>	<b>38</b>
5.1 物理安全控制.....	38
5.1.1 物理场地位置与建筑.....	38
5.1.2 物理访问.....	38

5.1.3 电力与空调.....	38
5.1.4 水患防治.....	39
5.1.5 火灾防护.....	39
5.1.6 介质存储.....	39
5.1.7 废物处理.....	39
5.1.8 异地备份.....	40
5.2 流程安全控制.....	40
5.2.1 可信角色.....	40
5.2.2 每项任务需要的人数.....	41
5.2.3 每个角色的识别与鉴别.....	41
5.2.4 职责分割原则.....	42
5.3 人员控制.....	42
5.3.1 资格、经历和无过失要求.....	42
5.3.2 背景审查程序.....	43
5.3.3 培训要求.....	43
5.3.4 再培训周期和要求.....	44
5.3.5 工作岗位轮换周期和顺序.....	44
5.3.6 未授权行为的处罚.....	45
5.3.7 独立合约人的要求.....	45
5.3.8 提供给员工的文档.....	45
5.4 审计日志程序.....	45
5.4.1 记录事件的类型.....	45
5.4.2 处理日志的周期.....	46
5.4.3 审计日志的保存期限.....	46
5.4.4 审计日志的保护.....	46
5.4.5 审计日志备份程序.....	46
5.4.6 审计收集系统.....	47
5.4.7 对导致事件实体的处理.....	47
5.4.8 脆弱性评估.....	47
5.5 记录归档.....	48
5.5.1 归档记录的类型.....	48
5.5.2 归档记录的保存期限.....	48
5.5.3 归档文件的保护.....	48
5.5.4 归档文件的备份.....	49
5.5.5 记录时间戳要求.....	49
5.5.6 归档收集系统.....	49
5.5.7 获得和检验归档信息的程序.....	49
5.6 电子认证服务机构密钥更替.....	49
5.6.1 密钥更替操作.....	49
5.6.2 密钥更替操作管理.....	50
5.7 损害与灾难恢复.....	50
5.7.1 事故和损害处理程序.....	52

5.7.2 计算资源、软件和/或数据的损坏.....	52
5.7.3 实体私钥损害处理程序.....	52
5.7.4 灾难后的业务连续性能力.....	53
5.8 电子认证服务机构或注册机构的业务终止.....	53
5.8.1 CA 终止原因.....	53
5.8.2 终止通知.....	53
5.8.3 终止归档.....	54
5.8.4 终止措施.....	54
5.8.5 RA 的终止.....	54
<b>6. 认证系统技术安全控制.....</b>	<b>55</b>
6.1 密钥对的生成和安装.....	55
6.1.1 密钥对的生成.....	55
6.1.2 私钥传送给订户.....	55
6.1.3 公钥传送给证书签发机构.....	55
6.1.4 CMCA 电子认证服务机构公钥传送给依赖方.....	56
6.1.5 密钥的长度.....	56
6.1.6 公钥参数的生成和质量检查.....	56
6.1.7 密钥使用目的.....	56
6.2 私钥保护和密码模块工程控制.....	57
6.2.1 密码模块的标准和控制.....	57
6.2.2 私钥多人控制.....	57
6.2.3 私钥托管.....	57
6.2.4 私钥备份.....	58
6.2.5 私钥归档.....	58
6.2.6 私钥导入、导出密码模块.....	58
6.2.7 私钥在密码模块的存储.....	58
6.2.8 激活私钥.....	59
6.2.9 解除私钥激活状态.....	59
6.2.10 销毁私钥.....	60
6.2.11 密码模块的评估.....	60
6.3 密钥对管理的其他方面.....	60
6.3.1 公钥归档.....	60
6.3.2 证书操作期和密钥对使用期.....	60
6.4 敏感数据.....	61
6.4.1 敏感数据的产生.....	61
6.4.2 敏感数据的保护.....	61
6.4.3 敏感数据的其他方面.....	61
6.5 计算机安全控制.....	62
6.5.1 具体的计算机安全技术要求.....	62
6.5.2 计算机安全评估.....	62
6.6 系统生命周期控制.....	63
6.6.1 系统开发控制.....	63

6.6.2 安全管理控制.....	63
6.6.3 生命周期的安全控制.....	63
6.7 网络的安全控制.....	63
6.8 时间戳.....	63
<b>7. 证书、证书吊销列表和在线证书状态协议.....</b>	<b>65</b>
7.1 证书.....	65
7.1.1 证书版本号.....	70
7.1.2 证书扩展项.....	70
7.1.3 算法对象标识符.....	72
7.1.4 名称形式.....	72
7.1.5 名称限制.....	74
7.1.6 证书策略对象标识符.....	74
7.1.7 策略限制扩展项的用法.....	75
7.1.8 策略限定符的语法和语义.....	75
7.1.9 关键证书策略扩展项的处理规则.....	75
7.2 证书吊销列表.....	75
7.2.1 版本号.....	75
7.2.2 CRL 和 CRL 条目扩展项.....	76
7.3 在线证书状态查询协议.....	76
7.3.1 版本号.....	76
7.3.2 OCSP 扩展项.....	77
<b>8 认证机构审计和其他评估.....</b>	<b>77</b>
8.1 审计的频率或情形.....	77
8.2 审计者的资质.....	77
8.3 审计者与中国移动 CMCA 的关系.....	78
8.3.1 审计者与中国移动 CMCA 的关系.....	78
8.4 审计内容.....	78
8.5 对问题与不足采取的措施.....	78
8.6 评估结果的传达与发布.....	78
8.7 其他.....	79
<b>9 法律责任和其他业务条款.....</b>	<b>79</b>
9.1 费用.....	79
9.1.1 证书签发和更新费用.....	79
9.1.2 证书查询费用.....	79
9.1.3 证书吊销或状态信息的查询费用.....	79
9.1.4 其他服务费用.....	79
9.1.5 退款策略.....	80
9.2 财务责任.....	80
9.2.1 保险范围.....	80
9.2.2 其他资产.....	80



9.2.3 对最终实体的保险或担保.....	81
如果 CMCA 根据本 CPS 或任何法律规定，以及司法判定须承担赔偿责任和/或补偿责任的， CMCA 将按照相关法律法规的规定、仲裁机构的裁定或法院的判决承担相应的赔偿责任。	
.....	81
9.3 业务信息保密.....	81
9.3.1 保密信息范围.....	81
9.3.2 不属于保密的信息.....	81
9.3.3 保护保密信息的信息.....	81
9.4 个人隐私保密.....	82
9.4.1 隐私保密方案.....	82
9.4.2 作为隐私处理的信息.....	82
9.4.3 不被视为隐私的信息.....	82
9.4.4 保护隐私的责任.....	82
9.4.5 使用隐私信息的告知与同意.....	83
9.4.6 依法律或行政程序的信息披露.....	83
9.4.7 其他信息披露情形.....	83
9.5 知识产权.....	83
9.6 陈述与担保.....	84
9.6.1 电子认证服务机构的陈述与担保.....	84
9.6.2 注册机构的陈述与担保.....	85
9.6.3 订户的陈述与担保.....	85
9.6.4 依赖方的陈述与担保.....	86
9.6.5 其他参与者的陈述与担保.....	86
9.7 担保免责.....	87
9.8 有限责任.....	87
9.9 赔偿.....	87
9.10 有效期限与终止.....	88
9.10.1 有效期限.....	88
9.10.2 终止.....	88
9.10.3 效力的终止与保留.....	88
9.11 对参与者的个别通告与沟通.....	88
9.12 修订.....	89
9.12.1 修订程序.....	89
9.12.2 通知机制和期限.....	89
9.12.3 必须修改业务规则的情形.....	89
9.13 争议处理.....	89
9.14 管辖法律.....	90
9.15 适用法律的符合性.....	90
9.16 一般条款.....	90
9.16.1 完整协议.....	90
9.16.2 转让.....	90
9.16.3 分割性.....	90

9.16.4 强制执行.....	91
9.16.5 不可抗力.....	91
9.17 其他条款.....	91

# 1. 概括性描述

## 1.1 概述

中国移动认证中心 (China Mobile Certification Authority, 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, 是经国家管理部门批准成立的第三方权威电子认证机构。

电子认证业务规则 (CPS, Certification Practice Statement) 是关于认证机构 (CA, Certification Authority) 在全部数字证书 (以下简称证书) 服务生命周期 (如签发、吊销、更新) 中的业务实践所遵循规范的详细描述和声明, 是对相关业务、技术和法律责任方面细节的描述。

中国移动证书信任体系 (CMTCN) 包括中国国内信任体系和全球信任体系, 本 CPS 是 CMCA 全球信任体系的证书业务规则声明, 根据国家相关法律法规的要求, 本 CPS 详细阐述了中国移动 CMCA 开展全球信任证书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。

本文档的编写遵从《中华人民共和国电子签名法》、中华人民共和国工业和信息化部颁布的《电子认证服务管理办法》、《电子认证业务规则规范 (试行)》, 以及最新的 RFC3647、《Webtrust 安全审计规范 2.0》、《EV 证书指导准则》以及《Baseline-Requirements》等。CMCA 遵循 <http://www.cabforum.org> 上发布的发布和管理公开的受信任证书基线要求的最新版本。

CMCA 已获得主管单位即工业和信息化部颁发的电子认证服务许可等资质, 并处于资质有效期内。

CMCA 全球信任体系遵循 WebTrust 相关要求, 并通过外部第三方审计机构审计。

本 CPS (V0.2) 的生效日期是 **2020 年 10 月 12 日**。

CMCA 全球信任证书体系的架构如下:

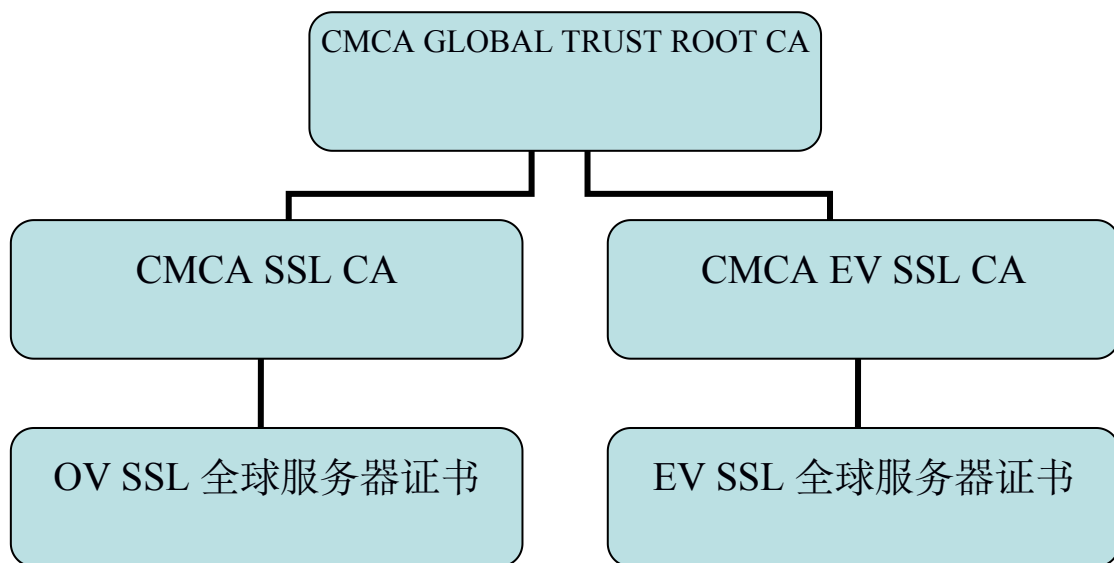


图 1 CMCA 全球信任全球信任证书体系架构

CMCA GLOBAL TRUST ROOT CA 根密钥长度为 4096-bit，有效期 25 年，将于 2045 年 10 月 16 日到期。

CMCA GLOBAL TRUST ROOT CA 下设两个中级根：

- CMCA SSL CA 根密钥长度为 4096-bit，有效期 20 年，将于 2040 年 10 月 16 日到期，签发普通 OV SSL 证书，订户证书有效期不超过 825 天。
- CMCA EV SSL CA 根密钥长度为 4096-bit，有效期 20 年，将于 2040 年 10 月 16 日到期，签发 EV SSL 证书，订户证书有效期不超过 825 天。

CMCA 中级根的生成遵循严格的管理规范，由授权人员执行特定操作签发。并经由第三方审计机构见证，中级证书的生成过程将全程记录，本 CPS 不做具体阐述。

## 1.2 文档名称与标识

### 1.2.1 名称

本文档中文名称为《CMCA 全球信任体系电子认证业务规则》（英文名《CMCA Global Trust CPS》）。

本文档策略对象标识号符（OID）为 1.2.156.711122.1.2.1。

OV SSL 证书对应的证书策略对象标识号符 (OID) 为 2.23.140.1.2.2。

EV SSL 证书对应的证书策略对象标识号符 (OID) 为 2.23.140.1.2.2。

## 1.2.2 版本

本 CPS 为首次发布版本，版本号为：V0.2。

## 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 CA (Certification Authority) 是颁发证书的实体，负责证书业务策略制定以及证书生命周期管理、密钥管理、信息库发布等工作，本文电子认证服务机构仅指 CMCA。

### 1.3.2 注册机构

注册机构 (Registration Authority, 简称 RA) 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。

CMCA 全球信任体系下的注册机构均设在 CMCA 内部，由 CMCA 本身承担 RA 职责，并未委托外部机构行使 RA 机构职责。

### 1.3.3 订户

订户是指向CMCA申请证书的实体。证书订户与证书主体是两个不同的概念。“证书订户”是指向CMCA申请证书的实体，通常为个人或机构；“证书主体”是指与证书信息绑定的实体，服务器证书中的“证书主体”通常是指受信任的服务器或用于确保与某一机构安全通信的其它设施。证书订户需要承担相应的责任与义务，而证书主体则是证书所要证明的可信赖方。

### 1.3.4 依赖方

依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的实体。

### 1.3.5 其他参与者

除 CMCA、订户和依赖方以外的参与者称为其它参与者。

## 1.4 证书应用

### 1.4.1 适合的证书应用

签发 CA	签发证书类型
CMCA SSL CA	OV SSL 全球服务器证书
CMCA EV SSL CA	EV SSL 全球服务器证书

CMCA GLOBAL TRUST ROOT CA仅用于签发中级CA证书，不签发最终订户证书。

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。

#### 1.4.1.1CMCA OV SSL全球服务器证书

CMCA OV SSL全球服务器证书包含通配符证书、多域名证书、单域名证书类型。该类证书适合用于在订户浏览器与Web服务器之间建立安全通道，实现数据信息在客户端与服务器之间的加密传输，防止数据信息的泄露。

CMCA OV SSL服务器证书（SHA256）由CMCA SSL CA签发SHA256证书，密钥长度为RSA-4096。

#### 1.4.1.2CMCA EV SSL全球服务器证书

CMCA EV SSL全球服务器证书包含单域名证书、多域名证书，该类证书适

合用于在订户浏览器与Web服务器之间建立安全通道，实现数据信息在客户端与服务器之间的加密传输，防止数据信息的泄露。

CMCA EV SSL全球服务器证书由CMCA EV SSL CA签发SHA256证书，密钥长度为RSA-4096。

## 1.4.2 限制/禁止的证书应用

CMCA全球信任体系下的证书根据其类型在功能上有所限制，比如EV SSL服务器证书只能用于经过严格认证的WEB服务器。

各类证书的密钥用法在订户证书中的扩展项中进行了限制。然而基于证书扩展项限制的有效性取决于应用软件，如果参与方不遵守相关约定，其对证书的应用超出本 CPS 限定的应用范围，将不受 CMCA 的保护。

CMCA 全球信任体系下签发的证书不能在如下领域使用：任何与国家或地方法律、法规规定相违背的应用系统。

## 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 CMCA 制定，并由该中心下设的全球信任认证策略委员会进行管理。

本 CPS 的策略文档管理机构为 CMCA 全球信任认证策略委员会，委员会下设工作组，当需要编写或修订本 CPS 时，由工作组组织编写，由委员会审批后正式发布。

### 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 CMCA 全球信任认证策略委员会，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：安全业务部

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：[cmca@aspirecn.com](mailto:cmca@aspirecn.com)

联络网站：[www.cmca.net](http://www.cmca.net)

### 1.5.3 决定 CPS 符合策略的机构

CMCA 全球信任认证策略委员会对本 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，CMCA 全球信任认证策略委员会将对提供的变动建议进行研究，做出变更决定。策略委员会至少每年一次组织对 CPS 内容进行审查，明确 CPS 是否要修订以及修订的内容，并组织工作组进行编写，经策略委员会批准后予以更新发布。

## 1.6 定义和缩写

CMCTN	中国移动证书信任体系 (China Mobile Certificate 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 Layer)
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

CMCA 信息库面向订户及证书应用依赖方提供信息服务。信息库包括但不限于以下内容：证书、CRL、CPS、CP、证书服务协议、技术支持手册以及 CMCA 网站信息等。

#### 2.1.1 信息库监督、监控机制

CMCA 针对信息库建立监督、监控机制：

1) 接口证书下载渠道：通过鉴权“证书申请请求 IP 地址”，确保接口请求来源可靠，

2) 网页证书下载渠道：通过定期下载测试证书，确保下载地址的可靠性。

以此保障信息库安全可靠，并确保信息库、分发库的证书和签发出的证书一致、订户获取的证书与签发证书一致，证书准确发放给了订户。

### 2.1.2 信息库内部数据维护

CMCA 将维护内部数据记录，用于记录所有曾经因为网络钓鱼可疑或可能被其他欺诈手段利用的原因被吊销或拒绝申请的证书信息（包括 EV 证书），这些证书的申请机构在今后的身份验证中标识为可能的高风险证书申请。

在进行身份验证时 CMCA 将申请机构与一些高风险机构名单进行比对，主要是指最有可能成为网络钓鱼或其他身份欺诈目标的组织机构，自动在申请阶段将其标记为“高风险申请者”，确保证书在签发前申请机构的身份得到充分验证。

这些组织名单有：

1) 参考国际反钓鱼工作组（APWG）及中国反钓鱼联盟（APAC）公布的钓鱼目标名单；

2) CMCA 将因为可能遭到网络钓鱼或其他身份欺诈攻击而吊销其 OV SSL 全球服务器、EVSSL 全球服务器证书，CMCA 将把这些被拒绝的申请者的组织机构标记为“高风险申请者”，并且作为今后识别高风险申请机构的依据。

CMCA 将拒绝处于高风险信息库中的证书申请。

## 2.2 信息发布

### 2.2.1 CPS 的发布

本 CPS 结构遵循 RFC 3647 且包含其要求的所有内容。

本 CPS 以及相关的技术支持信息等在 CMCA 网站上发布。

本 CPS 发布的内容为 CMCA 全球信任证书业务的基线要求，如有版本更新，以最新版本为准。

CMCA 遵循 <http://www.cabforum.org> 上发布的发布和管理公开的受信任证

书基线要求的最新版本。如果本文档和基线要求之间有任何不一致，基线要求优先于本文档。

### 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

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 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，至少每年对 CPS 进行审查一次，酌情进行更新。

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 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。

## 3. 身份标识与鉴别

### 3.1 命名

#### 3.1.1 名称类型

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域名、公网 IP 等，命名符合 X.500 定义的甄别名规范。

#### 3.1.2 对名称有意义的要求

DN (Distinguished Name)：唯一甄别名，在数字证书的主体名称域中，用于唯一标识证书主体的X.500名称，需要填写反映证书主体真实身份的、具有实际意义的、与法律不冲突的内容。

EV SSL全球服务器证书的甄别名称中的通用名只能是订户机构所拥有的域名，结合该订户机构的其他信息一起被鉴别和认证。

SSL 全球服务器证书的甄别名称中的通用名可以是订户所拥有的域名或者公网 IP，结合该订户的其他信息一起被鉴别和认证。

#### 3.1.3 订户的匿名或伪名

中国移动 CMCA 所签发的全球信任证书不可以使用匿名或伪名。

#### 3.1.4 理解不同名称形式的规则

DN (Distinguished Name) 的命名规则由 CMCA 定义，详见本 CPS 7.1.的说明。

### 3.1.5 名称的唯一性

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

### 3.1.6 商标的承认、鉴别和角色

CMCA 签发的证书的主体甄别名不包含任何商标或者可能对其他机构构成侵权的信息。

## 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

订户在申请CMCA全球信任体系签发的证书前，应提供有效机构身份证明文件、证书申请文件，并接受证书申请的有关条款，同意承担相应的责任。

CMCA 接受订户的证书申请后，应对订户的身份真实性进行审核，应使用可靠的数据源（所使用的数据源需经 CA 评估为可靠数据源，可靠数据源的评估包括信息所提供的信息、信息更新的频率、数据的收集和提供目的、数据可用性的公开可访问性、伪造和篡改相关困难）对订户身份的真实性进行审核，并按照双方的约定妥善保存订户申请材料。

CMCA对订户身份的鉴别过程如下：

业务受理人员收集订户的申请材料，并对订户身份以及材料进行线下审核。

RA操作员录入订户申请信息，RA审核员再次审核操作员录入信息并协助订户下载证书。

### 3.2.2.1 身份

订户如需要申请EVSSL或OVSSL全球服务器证书，可以向CMCA或者CMCA授权的代理机构提交申请，CMCA仅受理机构订户的申请。

EVSSL全球服务器证书只能是Web服务器的域名，并且域名不能包含通配符\*，不受理IP地址的申请，EVSSL全球服务器证书可以是单域名或多域名证书。

OVSSL 全球服务器证书可以包含单域名、多域名、通配符证书、公网 IP 证书。订户申请 EVSSL、OVSSL 全球服务器证书时，应提交如下材料：

	EV SSL 证书	OV SSL 证书
1	CMCA 全球信任体系证书申请表	
2	至少一种机构信息证明材料（特殊情况下需额外提供其他机构证件）	
3	证书申请文件（Certificate Signing Request, CSR 文件）	
4	律师函及律师资格文件，或其他根据 CA/B 论坛 EVSSL 证书鉴别要求中认可的补充文件	对应顶级域名的所有命名空间的控制权的有效证明或 CA/B 论坛认可的拥有公网 IP 的证明

CMCA除对申请者的身份、地址信息、国家信息等进行鉴别外，还要对域名、IP及CSR合规性进行鉴别。其鉴别要求、流程及方法如下：

#### 1、机构

- 企事业单位、组织、社会团队

- (1) 获得当地监管机构承认的合法组织，或获得当地政府的特许；
- (2) 监管机构认定的注册代表处或注册公司；
- (3) 不在组织/监管机构的“停业”、“无效”、“过期”、“失信”名单之列；
- (4) 至少有一个合法有效的授权代表；
- (5) 在订户申请材料中必须明确单位的授权代表；



- (6) 拥有固定的营业场所;
- (7) 机构注册或营业场所所在地法律允许CA签发证书的国家;
- (8) 不在中国的政府黑名单之列。

- 政府机构: 比如公安局、税务局等, 应满足以下条件:

- (1) 经由上级按照其职能批准建立;
- (2) 所在国家允许CA签发证书; (3) 不在中国的政府黑名单之列。

- 国际组织

(1) 由一国政府机构签署成立的私人基金、财团或等同机构。CAB论坛会维护可以申请EV证书的国际机构列表;

(2) 国际机构总部所在地必须允许CMCA从事电子认证业务或认可CMCA数字证书有效性;

(3) 国际机构不能在任何政府所列的禁止名单(如贸易禁运)上。其子机构或分支机构根据准则要求也可申请EV证书。

## 2、域名及IP

(1) 申请机构拥有EVSSL证书中的域名、OVSSL证书中的域名或公网IP的所有权或唯一使用权;

(2) 域名注册信息应公开在WHOIS数据库, 包括申请机构名称、地址和联系方式; 通过域名注册信息查询(whois)功能, 得到所申请域名证书的域名注册者资料, 查看域名注册者是否和域名证书申请者一致, 初步审核确定域名证书申请者确实拥有此域名。同时, CMCA将验证申请人对域名的所有权或控制权: 通过信函、传真、SMS或者邮递将一个随机值(有效期为从产生该随机值开始30天, 且在每个电子邮件、传真、短信或邮政邮件中是唯一的。)发送给域名联系人, 并收到使用该随机值的确认回复

如申请证书的域名与知名网站域名比较相似、或含有知名商标, 则CMCA会进行多层审查, 并通过高风险信息库进行比对, 以防止相似欺诈域名申请证书。

对于公网IP的鉴别, 通过信函、传真、SMS或者邮递将一个随机值(有效期为从产生该随机值开始30天, 且在每个电子邮件、传真、短信或邮政邮件中是唯一的。)发送给IP地址联系人, 并收到使用该随机值的确认回复, 以验证申请人对IP地址的控制权。

如果申请通配符域名证书, CMCA将鉴别其拥有的二级域名。对于多域名证书, CMCA将对所有列举的域名进行鉴别。

## 3、申请机构角色

申请单位需要如下的角色:

- ✓ 申请经办人：申请单位经办人员
- ✓ 申请确认人：申请单位的主管人员，确认申请信息的准确性和有效性

证书申请机构可授权一个人来完成所有的角色，也可以分别让多个人来完成。以上角色必须是申请单位的职员或被授权的代理人，申请单位需确认申请角色的信息真实准确并以CMCA认可的方式（包括但不限于注册公章、注册法人人名章、角色手印等方式）进行声明，对于不实的申请角色信息，CMCA有权拒绝申请，并对已发放的证书进行吊销。

个人身份的认证：居民身份证、护照等。

#### 4、CSR符合性鉴别

对于CSR文件的鉴别主要包含，CSR中的信息是否与申请表中的申请信息一致，是否符合相关规范，比如DN的顺序等，并验证其是否拥有私钥。

#### 5、EVSSL、OVSSL全球服务器证书公钥证书分发

CMCA为订户签发公钥证书，并以邮件方式将签发的公钥证书交付给订户。

### 3.2.2.2 DBA/商业名称的鉴别

若证书主题中包含 DBA 或商业名称，CMCA 将通过以下方式中的至少一种确认申请者有权使用该 DBA 或商业名称。

- (1) 政府机构提供的可证明申请者合法成立、存在或认可的有效文档
- (2) 可靠的数据来源（如邓白氏编码、商务部对外贸易经营者备案）
- (3) 其他CMCA认为可靠的验证方式。

### 3.2.2.3 国别验证

若证书主题中包含国家选项，CMCA将通过以下方式中的至少一种进行国家的鉴别。

- (1) 通过权威第三方数据查询网站DNS记录显示的IP地址或申请者的IP地址来确认所在国家，确保申请人的IP地址所在国与申请



人实际所在国一致。

- (2) 请求域名的ccTLD
- (3) 域名注册机构提供的信息
- (4) 通过本文第3.2.2.1节种申请者提供的机构证明信息所在国家的确认。

#### 3.2.2.4 域名的确认和鉴别 Verification and Authentication of Domain

对于域名的验证, 被验证的实体可以是申请者的母公司、子公司或联营公司, CMCA将采用以下鉴别方式中的一种, 确认申请者拥有该域名。

- (1) 参照第3.2.2.9节中邮件地址的确认和鉴别方法, 通过邮件方式发送随机值, 然后接收一个使用该随机值的确认响应, 确认申请人对FQDN的所有权。随机值必须发送到WHOIS注册备案的域名联系人电子邮件地址。(根据Baseline Requirements v1.7.6第3.2.2.4.2的域名验证方法)
- (2) 参照第3.2.2.9节中邮件地址的确认和鉴别方法, 通过邮件方式发送随机值, 然后接收一个使用该随机值的确认响应, 确认申请人对FQDN的所有权。随机值必须发送到标识为域名联系人的电子邮件地址 'adimn', 'adimnistrator', 'webmaster', 'hostmaster' 或 'postmaster', 后面是 ( “@” ) 之后跟着授权域名。(依据Baseline Requirements v1.7.6 第3.2.2.4.4的域名验证方法)
- (3) 通过在 “/.well-known/ pki-validation” 目录下对约定的信息进行改动, 确认订户对FQDN的所有权。(依据Baseline Requirements v1.7.6 第3.2.2.4.18的域名验证方法)
- (4) 通过在DNS CNAME、TXT或CAA记录中是否存在已约定的随机值, 以确认订户对域名的所有权。要求: 1) 授权域名; 或者2) 一个前缀以下划线字符开头的域名授权。(依据Baseline Requirements v1.7.6 第3.2.2.4.7的域名验证方法)

上述验证方法中用到的随机值有效期为从产生该随机值开始的30天。

CMCA不为.onion形式的域名签发SSL全球服务器证书。

### 3.2.2.5 IP 地址的验证

组织机构如向 CMCA 申请全球服务证书, CMCA 将验证申请人对 IP 地址的所有权或控制权, IP 地址控制权验证方法使用如下方式:

通过信函、传真、SMS 或者邮递将一个随机值 (有效期为从产生该随机值开始 30 天, 且在每个电子邮件、传真、短信或邮政邮件中是唯一的。) 发送给 IP 地址联系人, 并收到使用该随机值的确认回复, 以验证申请人对 IP 地址的控制权, 按照 BR 章节 3.2.2.5.2 执行。

### 3.2.2.6 通配符域验证

对于通配符 “\*” 右侧直接接顶级域名的申请, 除非申请者能够有效证明其对于该顶级域名的所有命名空间的控制权, 否则 CMCA 将拒绝该类申请。同时, 将通过 3.2.2.4 中的鉴别方式来核实通配符右侧的域名确实已被有效注册, 并归属于该申请者。

### 3.2.2.7 数据源的准确性

CMCA 采用准确、可靠的第三方数据源来验证证书申请者的信息。在选择是否依赖一个数据源之前, CMCA 会对该数据源的可依赖性、数据的准确性以及数据的抗更改和抗伪造性进行评估。将考虑以下几个方面:

- 1) 所提供的信息的年限;
- 2) 该数据源更新的频率, 确保数据保持更新;
- 3) 数据的供应方, 以及数据收集的目的;
- 4) 数据的公开可用性及可访问性;
- 5) 伪造或更改数据的难度。

对于 SSL 证书的验证数据源, 若获得可依赖数据或文件的时间不超过 825 天, 则可复用。

### 3.2.2.8 CAA 记录

**CMCA 依照 RFC 8659 的要求进行 CAA 记录验证。**

订户向 CMCA 申请全球信任证书, CMCA 会查询订户是否有指定的 CA 机构, 具体通过查询 CAA 公开数据来判断, 如果订户有指定 CA 机构, 则 CMCA

将不再受理证书申请；反之，CMCA 正常受理证书业务申请。如果签发证书，必须在 CAA 记录的 TTL 时间或 8 小时内（两者更大者）。

### 3.2.3 个人身份的鉴别

CMCA 不受理个人证书业务，此部分要求仅针对企业申请授权办理人员的身份鉴别。中国移动 CMCA 将核对证书申请人信息与提供的身份证信息是否一致，并将数字证书申请人身份证复印归档备案。

### 3.2.4 没有验证的订户信息

CMCA 签发的证书信息没有未经过验证的信息。

### 3.2.5 授权确认

当申请者代表组织机构订户申请证书时，需要出示足够的证明信息以证明申请者是否已获得组织机构的授权。CMCA 有责任确认该授权信息，并将授权信息妥善保存。

当机构授权经办人办理证书业务时，应当进行的核实验证流程参照本 CPS 相关要求。

CMCA 允许申请者指定独立个人来申请证书。若申请者以书面形式指定证书申请人，则不接受在该指定人员以外的其他人提交证书申请请求。在收到申请者确认的书面请求时，应向申请者提供其已授权人员的清单。

### 3.2.6 互操作准则

对于申请 CMCA 全球信任体系下的 OV 证书及 EV 证书，CMCA 承担对订户身份的鉴别职能，暂不委托其他机构行使此职责。

CMCA 不涉及任何交叉认证业务，为签发任何交叉认证的证书。

### 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。证书更新请求包含“密钥更新”和“证书更新”，对于密钥更新而言，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，具体参考（同 4.7）；对于“证书更新”，CMCA 暂不支持该服务，客户申请更新证书时，需重新填写证书更新表，按照初始身份验证步骤提交相关资料（同 4.1），并由中国移动 CMCA 或其授权机构审核。

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 签发证书有效期一般为 1-2 年，有效期不超过 825 天。

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。

#### 3.3.2 吊销后更新的标识与鉴别

吊销后的证书必须重新生成新的公私钥对并按照 3.2 的规定申请新的证书。

## 3.4 吊销请求的标识与鉴别

### 3.4.1 证书吊销情况

订户本人申请吊销证书，其身份鉴别使用初始身份确认相同的流程，详见 3.2。

如果是 CMCA 主动发起吊销，如订户没有履行本 CPS 所规定的义务，则不需要对订户身份进行标识和鉴别。由 CA\RA 发出的吊销操作应有相应的 request 记录能够标识出是由 CA\RA 主体发起的吊销。

### 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。

## 4. 证书生命周期操作要求

### 4.1 证书申请

#### 4.1.1 证书申请实体

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

#### 4.1.2 注册过程与责任

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

申请者应向 CMCA 递交证书申请表及相应证明文件，此行为即意味着申请者已经了解和接受订户协议。

##### 1、最终订户

最终订户即申请证书的实体，最终订户须明确表示其愿意接受本CPS及相关的CP中所规定的相关责任与义务（本CPS及相关CP公布在CMCA网站上），并需要按照3.2.2的要求提供真实、准确的申请信息；根据《中华人民共和国电子签名法》的规定，申请者未向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、CMCA或者CMCA授权的代理机构造成损失的，订户应承担相应的法律及赔偿责任。订户有责任保护其拥有的证书私钥安全。

##### 2、认证及注册机构

对于全球信任体系证书，CMCA既是一个CA，同时也承担了注册机构的职能，如订户可以直接向CMCA申请证书，由CMCA审核订户信息并处理订户的请求。注册机构对订户提供的身份信息参照3.2.2的要求进行鉴别，CMCA对通过鉴别后的订户签发证书。CMCA作为电子认证机构，应妥善保管证书订户申请信息。CMCA授权的代理机构应在适当时间将证书订户的信息归档在CMCA，同时应履行本CPS中所规定的相关责任与义务。



## 4.2 证书审核

### 4.2.1 执行识别与鉴别功能

1. CMCA 处理证书申请至少需要设置 3 个可信角色：信息收集、信息验证、签发证书。其中信息收集、信息验证可以由同一人完成；但签发证书人员需要与信息收集、信息验证职责分离。

2. 对于证书申请处理，签发证书人员需对申请机构信息做最终审核：

1) 对所有用以验证申请机构证书申请的信息和文件进行复核，查找冲突的信息或需要进一步验证的信息；

2) 如复核人提出的问题确实需要得到进一步验证，CMCA 必须从申请机构、协议签署人、申请审批人或其他合格的独立信息来源取得进一步验证的资料或证据；

3) CMCA 必须保证已收集的与证书申请相关的信息和资料，足以确保签发的证书不包含 CMCA 已知或应发现的错误信息，否则 CMCA 将会拒绝证书的申请并通知申请机构；

4) 如果部分或所有的身份验证资料内容使用语言不是 CMCA 的官方语言，那么 CMCA 将会使用经过适当的培训、具备足够的经验和判断能力的人员完成最终的交叉审核和尽职调查。CA 通过以下方法执行交叉审核与尽职调查：

4.1) 依赖翻译的材料内容；

4.2) 依赖拥有此语言能力的代理机构完成此步骤，CMCA 复核代理机构的检查结果，并且复核证书标准中的 CMCA 自我审核要求。

5) 根据 CA/BForum 的相关指引，CMCA 在执行识别和鉴别职责时，将对客户提交的域名信息进行 CAA 查询，CMCA 会查询订户是否有指定的 CA 机构，具体通过查询 CAA 公开数据来判断，如果订户有指定 CA 机构，则 CMCA 将不再受理证书申请；反之，CMCA 正常受理证书业务申请。如果签发证书，必须在 CAA 记录的 TTL 时间或 8 小时内（两者更大者）。

并在审核记录中体现。

CMCA 建立高风险证书请求额外验证机制：

1. 建立高风险申请人列表，获取信息的渠道包括但不限于反钓鱼联盟、防病毒厂商、负责网络安全事务的政府机构、媒体的公开报道等；
2. 对于出现在高风险申请人列表的机构，CMCA 有权直接拒绝证书申请或请其提供额外的验证材料，

对于已签发的证书也应定期根据高风险申请人列表进行复核，如出现在列表中，并采取适当行动 CMCA 有权直接吊销证书申请或请其提供额外的验证材料。

## 4.2.2 CMCA 证书申请批准和拒绝

CMCA将在合理的时间内完成证书申请处理。在申请提交的资料齐全且审核通过的情况下，1-3个工作日处理完成。EVSSL全球服务器证书处理证书申请时间不超过5个工作日，特殊情况最长不超过10个工作日。

CMCA拒绝签发包含内部名称的证书。

CMCA拒绝签发包含匿名、伪名证书。

## 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，CMCA 在 3 个工作日内完成证书申请的处理，EV SSL 全球服务器证书处理证书申请时间不超过 5 个工作日，特殊情况最长不超过 10 个工作日。

## 4.3 证书签发

### 4.3.1 证书签发中注册机构和电子认证服务机构的行为

CMCA 在订户申请通过鉴别后，RA 系统操作员录入订户申请信息，并提交 RA 系统审核员审核；RA 系统审核员审核通过后，向 CA 系统提交申请；CA 系统向 RA 系统返回证书，由 CA 以安全的形式将证书反馈给订户。



### 4.3.2 电子认证服务机构和注册机构对订户的通告

CMCA 无论是拒绝还是批准订户的证书申请，CMCA 有义务告知订户申请结果。CMCA 会以电话、电子邮件或其他方式对订户进行通告。

## 4.4 证书接受

### 4.4.1 构成接受证书的行为

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，应妥善保管其证书对应的私钥。

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) 证书申请者是最終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。

## 4.4.2 电子认证服务机构对证书的发布

对于最终订户证书，CMCA将根据用户的意愿采取适当形式的发布；订户没有要求发布的，CMCA将不发布最终订户证书。

## 4.4.3 CMCA 对其他实体的通告

对于CMCA签发的证书，CMCA不对其他实体进行通告，依赖方可以在信息库上自行查询。

# 4.5 密钥和证书的使用

## 4.5.1 订户私钥和证书的使用

订户的私钥和证书应用于规定的、批准的用途（在本CPS1.4.1节定义），订户在使用证书时必须遵守本CPS的要求，妥善保管其私钥，避免他人未经本人授权而使用本人证书情形的发生，否则其应用是不受保障的。

### 1、证书持有者的公钥和证书使用

证书持有者只能在指定的应用范围内使用私钥和证书，证书持有者只有在接受了相关证书后才能使用对应的私钥，并且在证书到期或被吊销后，须停止使用该证书及对应的私钥。预植证书及对应的私钥只有在该证书被绑定激活后才能使用。

### 2、依赖方的公钥和证书使用

当依赖方接受到签名的信息后，应该：

- ◆获得对应的证书及信任链；
- ◆验证证书的有效性；
- ◆确认该签名对应的证书是依赖方信任的证书；
- ◆证书的用途适用于对应的签名；令使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。

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

## 4.5.2 依赖方公钥和证书的使用

依赖方信赖CMCA全球信任体系签发的证书所证明的信任关系时需要：

- 1、获取并安装该证书对应的证书链；
- 2、在信赖证书所证明的信任关系前确认该证书为有效证书，包括：检查CMCA公布的最新CRL，或者通过CMCA提供的OCSP服务确认该证书未被吊销；检查该证书路径中所有出现过的证书的可靠性；检查该证书的有效期；以及检查其他能够影响证书有效性的信息；
- 3、在信赖证书所证明的信任关系前确认该证书记载的内容与所要证明的内容一致。

## 4.6 证书更新

CMCA不提供全球信任证书更新服务。

### 4.6.1 证书更新的原因

不适用

### 4.6.2 请求证书更新的实体

不适用

### 4.6.3 证书更新流程

不适用

### 4.6.4 颁发新证书时对订户的通告

不适用

## 4.6.5 构成接受更新证书的行为

不适用

## 4.6.6 电子认证服务机构对更新证书的发布

不适用

## 4.6.7 电子认证服务机构对其他实体的通告

不适用

## 4.7 证书密钥更新

证书密钥更新是指订户生成新的密钥对并申请为新公钥签发新证书 CMCA。

### 4.7.1 证书密钥更新的情形

- 1、当订户证书密钥遭到损坏时；
- 2、当订户证实或怀疑其证书密钥不安全时；
- 3、其它可能导致密钥更新的情形。

### 4.7.2 请求证书密钥更新的实体

已经申请过 CMCA 证书的订户可申请证书密钥更新。

### 4.7.3 证书密钥更新请求的处理

同 3.3。

### 4.7.4 颁发新证书时对订户的通告

同 4.3.2。

## 4.7.5 构成接受密钥更新证书的行为

同 4.4.1。

## 4.7.6 电子认证服务机构对密钥更新证书的发布

通过证书 Rekey，订户可以获得一个新的证书来替换一个旧的证书，新证书需要满足如下条件：

- 1.包含与旧证书相同的信息(身份、域名等)
- 2.与旧证书相同的有效日期(而不是延后的日期)
- 3.包含与旧证书不同的公钥

## 4.7.7 电子认证服务机构对其他实体的通告

同 4.4.3。

# 4.8 证书变更

## 4.8.1 证书变更的原因

不适用

## 4.8.2 请求证书变更的实体

不适用

## 4.8.3 证书变更的流程

不适用

#### 4.8.4 颁发新证书时对订户的通告

不适用

#### 4.8.5 构成接受变更证书的行为

不适用

#### 4.8.6 电子认证服务机构对变更证书的发布

不适用

#### 4.8.7 电子认证服务机构对其他实体的通告

不适用

### 4.9 证书吊销和挂起

#### 4.9.1 证书吊销的情形

如有下列情况中的任何一种情况发生，则订户的证书将被吊销：

- 1) 订户书面申请吊销数字证书；
- 2) 订户通知CA最初的证书申请未经有效授权；
- 3) 订户相信或怀疑密钥泄漏或遭受攻击，存放证书的服务器损坏或被锁定等情形；或者CA有证据表明订户证书私钥泄露的情形；
- 4) CMCA获知已出现了经过验证的订户私钥泄露方法，该方法可基于公钥很容易地计算出订户私钥（例如 Debian 弱密钥，请参阅 <http://wiki.debian.org/SSLkeys>）；
- 5) CA机构获得证据，证书中所包含的域名或IP地址的控制权验证已不再可靠；
- 6) C机构收到通知或以其他方式得知任何表明订户不再合法使用证书中电子邮件地址的情况。

CA 应该在 24 小时内撤销证书，如有下列其中一项或多项，必须在 5 天内撤销证书：

1. 证书不再符合 Mozilla Root Store Policy 或 CA/Browser 论坛的 Baseline 第 Requirements 中第 6.1.5 及 6.1.6 节的规定；
2. CA 取得证书被滥用的证据；
3. CA 获悉订户已违反订户协议或使用条款项下的一项或多项重要义务；
4. CA 机构得知订户不再能合法使用证书中包含的域名或 IP 地址，如法院或仲裁停止了域名注册商使用某域名的权限，或域名注册商与申请人之间的使用许可或服务协议终止了
5. CA 了解到某通配符证书被用于验证具有欺诈误导性质的域名
6. CA 获悉证书所载的信息有重大改变
- 7 发现并证实某证书没有根据 CA/浏览器论坛（CA/Browser Forum）发布的最新版本的 Guidelines 、 Baseline Requirement 以及 CP、CPS 要求的程序而签发
8. CA 确定或知悉证书内的任何信息不准确
9. CA 签发证书的权利已届满或被撤销或终止，除非 CA 已作出安排，继续维护 CRL/OCSP；
10. CA 的 CP 及/或 CPS 规定撤销证书；
11. 证书的技术内容或格式造成了对应用软件供应商或依赖方不可接受的风险，如 CA/浏览器论坛决定弃用某种算法或密钥长度，认为其风险水平不可接受，在一定期限内 CA 应撤销此类证书

#### 撤销下级 CA 证书的情形

若发生下列一种或多种情况，签发 CA 应在七(7)天内撤销下级 CA 证书：

1. 下级核证机关要求书面撤销；
2. 下级 CA 通知签发 CA，原来的证书请求没有得到授权，并且没有后续补充授权；
3. 签发 CA 取得证据，证明其所属 CA 与证书上的公钥对应的私钥发生了密钥泄露或不再符合第 6.1.5 和 6.1.6 条的要求；
4. 签发 CA 取得证书被滥用的证据；
5. 签发 CA 意识到证书不是按照 CA/浏览器论坛（CA/Browser Forum）发



布的最新版本的 Guidelines 、 Baseline Requirement 以及 CP、CPS 要求签发的，或者下级 CA 没有遵守 CA/浏览器论坛 (CA/Browser Forum) 发布的最新版本的 Guidelines 、 Baseline Requirement 以及 CP、CPS 要求

6. 签发 CA 确定证书所载的任何信息不准确或有误导性;

7. 签发 CA 或附属 CA 因任何理由而停止运作，并没有安排其他 CA 为该证书提供撤销支持

8. 签发 CA 或下级 CA 签发证书的权利已届满或被撤销或终止，除非 CA 已作出安排，继续维护 CRL/OCSP;

9. 签发 CA 的 CP 及/或 CPS 规定撤销证书;或

### 4.9.2 请求证书吊销的实体

可要求撤销证书的实体包括：订阅者、RA、CA、法院、政府主管部门及其他公权力部门。此外，订阅者、依赖方、应用软件供应商和其他第三方可以通过在线提交或者邮件等方式（详见 [www.cmca.net](http://www.cmca.net) 官网联系方式）提交证书问题报告，通知发出证书的 CA 撤销证书的合理原因。

同时，CMCA也可在4.9.1所述的情形下主动吊销订户的证书。

### 4.9.3 吊销请求的流程

CMCA提供724稳定的系统服务，可以实时接受和响应证书吊销请求和证书问题报告。订阅者、依赖方、应用软件供应商和其他第三方如发现或怀疑证书存在问题，可以通过CMCA官网及时报告，包括但不限于以下情形可疑的私钥泄漏、证书误用或其他类型的欺诈、折衷、误用、不当行为或与证书相关的任何其他事项。

吊销分为主动吊销和被动吊销。主动吊销是指订户提出吊销申请，由CMCA审核通过后吊销证书的情形；被动吊销是指当CMCA确定订户违反证书使用规定、约定、或是订户主体已经消亡等情况发生时，采取吊销证书的手段已停止对该证书的证明。

#### 4.9.3.1 主动吊销



订户申请吊销证书前应指定并书面授权证书吊销申请代表, 提供有效身份证明文件及证书吊销申请文件, 并接受证书吊销申请的有关条款, 同意承担相应的责任。

CMCA 7\*24 接受订户证书吊销申请, 并处理订户证书吊销请求。

CMCA 收到订户的吊销申请材料后, 将查询订户需吊销的证书是否为 CMCA 所发放, 证书是否在有效期内, 吊销理由是否属实, 若均通过则对证书进行吊销。

#### 4.9.3.2 被动吊销

当出现被动吊销的情形时, CMCA 将以适当形式通知订户, 告知拟吊销的证书内容、吊销原因、吊销操作时限等事项, 在确认订户收到吊销通知且无异议后予以吊销。

CMCA 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, 无需用户提出吊销申请。

- 证书的私钥泄漏
- 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 CMCA 或其授权的注册机构根据 CA 策略对客户的证书执行吊销操作时, 须按照如下流程进行:

- 中国移动 CMCA 或授权的注册机构或受理点书面填写“证书吊销申请表”, 并附上必须吊销证书的问题报告;
- 中国移动 CMCA 或授权的注册机构按照第三章的要求对等待吊销的证书申请进行审核;
- 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以及吊销原因;
- 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。

依赖方和其他第三方, 有责任和义务向 CMCA 报告可疑的私钥泄漏、证书误用或其他类型的欺诈、折衷、误用、不当行为或与证书相关的任何其他事项。

## 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。订户申请吊销时，RA 应在收到吊销请求 24 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

在主动吊销的情形下，CMCA 收到吊销请求并审核完成后，24 小时内吊销证书。

在被动吊销的情形下，订户在收到吊销通知后的 3 个工作日内可向 CMCA 提出申辩理由，CMCA 将会对申辩理由进行评估，若确认其理由正当则不予以吊销；若订户在 3 个工作日内未回复或回复无异议，则 CMCA 将于 24 小时内予以吊销。

a. 应向订户、依赖方、应用软件供应商和其他第三方提供明确指示，以报告可疑的私钥泄漏、证书误用或其他类型的欺诈、折衷、误用、不当行为或与证书相关的任何其他问题事项。

b. 应识别高优先级证书问题报告。

c. 在收到证书问题报告后 24 小时内，应调查与证书问题报告有关的事实和情况，并向订户和提交证书问题报告的实体提供初步调查报告。

在审查事实和情况后，应与订户和报告证书问题报告或其他与撤销有关通知的任何实体一起确定是否要撤销证书，如果要撤销证书，应确定撤销证书的日期。从收到证书问题报告或与撤销有关的通知到公布撤销的时间不得超过第 4.9.1.1 条规定的期限。选择撤销日期时应考虑下列原则：

- 所指称问题的性质(范围、背景、严重程度、程度、损害的风险)；
- 撤销的后果(对订阅者和依赖方的直接和间接影响)；
- 收到的有关特定证书或用户的证书问题报告的数量；
- 提出投诉的实体(例如，执法人员对网站从事非法活动的投诉应比消费者对其未收到所订购商品的投诉更有分量)；

- 相关法律法规。

d.应保持连续的 24x7 能力，对高优先级证书问题报告进行内部响应，并在适当情况下，将此类投诉提交给执法部门，并/或撤销此类投诉所涉及的证书。

#### 4.9.6 依赖方检查证书吊销的要求

依赖方在信任此证书前应检查证书的有效性，确认证书未被吊销。

#### 4.9.7 CRL 发布频率

订户证书的 CRL 在 24 小时内更新；订户有特殊要求的，将根据订户的需求，适当更新 CRL 发布的频率。CMCA 签发的 CRL 信息，根据需要，也可以人工方式实时发布。

CMCA 提供 CRL 服务，响应时间小于 10 秒。

中级 CA 证书的 CRL 发布频率：

CMCA 每 12 个月更新和补发 CRLs 一次(i)，在撤销中级 CA 证书后的 24 小时内更新和补发 CRLs 一次(ii)。

CMCA 确保在证书有效期结束前，证书的吊销状态可以在 CRL 中被查询。

#### 4.9.8 CRL 发布的最大滞后时间

CMCA 的 CRL 发布的最大滞后时间为 24 小时。

#### 4.9.9 在线状态查询的可用性

OCSP 服务网址 <https://mpus.cmca.net:8080/ocsp>

CMCA 提供 OCSP 查询服务，服务 7\*24 小时可用。CMCA 的 OCSP 响应符合 RFC6960 标准。CMCA 确保在证书有效期结束前，证书的吊销状态可以在 OCSP 中被查询。

信赖方是否进行在线状态查询完全取决于信赖方的安全要求。对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，信赖方在信赖一个证书前可通过证书状态在线查

询系统检查该证书的状态。

客户通过 http 协议访问 CMCA 的 OCSP 服务，CMCA 会对查询请求进行检查，检查的内容包括：

- ◆验证是否强制请求签名
- ◆用 CA 证书验证签名是否通过
- ◆验证证书是否生效或者已经过期
- ◆验证证书颁发者是否在信任证书列表内

OCSP 响应包含下表所属的基本域和内容

域	值或者值的限制
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。Sha1RSA 算法签名
颁发者	签发 OCSP 的实体。签发者公钥的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、证书状态以及证书废止信息
证书标识	包括数据摘要算法、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。
证书废止信息	当返回证书状态为废止时包含废止时间和废止原因

OCSP 的扩展信息与RFC6960一致。

#### 4.9.10在线状态查询要求

CMCA 能够提供在线状态查询，证书订户和依赖方可通过 OCSP 服务进行证书状态的实时查询。

OCSP 所有返回的信息均已电子签名，并包括所有所需的数据。

中国移动CMCA提供的OCSP服务支持GET方式。

对于中级证书及订户证书而言 CMCA 的 OCSP 信息的更新频率为 10 小时；OCSP 服务响应最大时间为 10 秒；OCSP 服务响应信息最大有效期为 10 小时。

#### 4.9.11 吊销信息的其他发布形式

证书吊销信息可以通过CRL或者OCSP服务获得。订户可通过证书扩展域中的CRL地址获得CRL信息。

#### 4.9.12 密钥损害的特别要求

无论是订户还是 CMCA，发现或者怀疑密钥安全被损害时，应该立即吊销证书，并发布到 CRL。吊销后如需继续申请证书，按照证书申请流程进行操作。

#### 4.9.13 证书挂起的情形

CMCA 不提供全球信任证书的证书挂起服务。

#### 4.9.14 请求证书挂起的实体

CMCA 不提供全球信任证书的证书挂起服务。

#### 4.9.15 挂起请求的流程

CMCA 不提供全球信任证书的证书挂起服务。

#### 4.9.16 挂起的期限限制

CMCA 不提供全球信任证书的证书挂起服务。

## 4.10 证书状态服务

### 4.10.1 操作特性

证书状态可以通过CMCA提供的OCSP 以及CRL 获取（在证书到期之前）上述方式的证书状态服务应该对查询请求有合理的响应时间和并发处理能力。证书吊销信息的保留期限至证书有效期后。

### 4.10.2 服务可用性

中国移动CMCA提供7\*24小时不间断OCSP（在线证书状态查询）服务，在网络允许的情况下，订户能够实时获得证书状态查询服务，响应时间小于10秒。

### 4.10.3 可选特征

无。

## 4.11 订购结束

订购结束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，服务终止自动产生。
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，如用户申请吊销该证书。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

## 4.12 密钥托管与恢复

### 4.12.1 密钥恢复的策略与行为

不适用。CMCA不托管任何SSL证书订户的私钥，因此也不提供密钥恢复服务。

## 4.12.2 会话密钥的封装与恢复的策略与行为

不做规定。



## 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。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 物理场地位置与建筑

CMCA的运营机房位于广东省广州市天河区高唐路333号中国移动南方基地数据中心B座5楼，进入机房须经过三道审核，机房电磁屏蔽效能满足GJBz20219-94标准“C”级要求。机房具备抗震、防火、防水、恒湿温控、独立供电、备用发电、门禁控制、视频监控等功能，可保证认证服务的连续性和可靠性。

#### 5.1.2 物理访问

外来人员进入CMCA机房，需经过中国移动南方基地、CMCA两道审核，进入CMCA机房需要有CMCA工作人员陪同进入。

操作人员进入CMCA综合机房，须经过指纹认证加门禁授权卡身份认证，并有24小时视频监控设备进行监控。

操作人员进入安全区机房，须经过三道门禁系统，其中两道是双人指纹加门禁卡认证，一道是双人门禁卡认证，并且所有门禁的进出信息都会在监控室的安保系统中记录。

#### 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

CMCA 保管的介质是指光盘、硬盘、软盘、U 盘、存储卡、磁带等，由专人管理，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。

敏感的文件资料 (包括纸介质、光盘或软盘废物等) 抛弃前要进行粉碎处理; 对于存储或传输信息的介质, 在抛弃前要做不可读取处理; 涉密介质在抛弃前要根据生产商的指导做归零处理。加密机等重要设备废弃根据加密机管理办法销毁。

### 5.1.8 异地备份

CMCA建立了异地备份机制。

- 设置异地备份机房, 并配置相关设备, 当 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。
- 。
- 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。

#### 5.1.9 时间戳服务器证书物理控制

CMCA独立控制并运营时间戳服务器, 其密钥保存在加密机中, CMCA确保时间戳服务使用的私钥被保存在符合FIPS-140-2级别或者更高级别的加密机中, CMCA时间戳服务提供的时间源为北斗时, 溯源自中国科学院国家授时中心协调时间时UTC。

## 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。

在物理安全的环境中, CA 私钥必须由受信任角色的人员至少使用双重控制进行的活动应当添加备份与存储。

### 5.2.3 每个角色的识别与鉴别

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 and 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。对任何参与证书管理过程的人员，无论是作为 CA 的雇员、代理或独立合约人，CA 中心都应核实该人员的身份和可信度。

### 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

中国移动 CMCA 对录用人员按照其岗位和角色安排培训。培训内容有：PKI 的相关知识、岗位职责、内部规章制度、认证系统软件、相关应用软件、操作系统与网络、ISO9000 质量控制体系、ISO27001 信息安全管理体系、CPS 等。

处理证书业务相关的员工必须接受下列培训：

- 1)向所有负责信息身份验证的职员（“验证专家”）提供技能培训。培训内容包括基础 PKI 知识、审核与验证制度和流程、对验证过程的主要威胁因素（如，网络钓鱼及其他社会工程学策略）；
- 2)保留人员培训记录，并且确保“验证专家”能够胜任身份信息验证工作的技术要求；
- 3)验证专家必须按其不同的技术水平等级被授予不同的签发证书权限，技术水平分级标准应与培训内容以及业绩考核标准一致；
- 4)确保为验证专家分配签发证书权限前，不同技术水平等级的验证专家都具有足够的胜任能力；
- 5)要求所有的验证专家通过关于证书标准中身份验证要求的 CA 内部考试。

### 5.3.4 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受 CMCA 组织的培训一次。

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。

中国移动 CMCA 所有受信任角色的人员应保持与 CA 的培训和绩效计划一致的技能水平。

### 5.3.5 工作岗位轮换周期和顺序

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。

CMCA 根据具体工作情况安排并制定员工工作岗位的轮换周期与顺序。



### 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 独立合约人的要求

CA 应验证授权的第三方人员在证书颁发过程中是否符合第 5.3.3 节的培训和技能要求，以及第 5.4.1 节的文件保存和事件记录要求。

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

1. 人员档案进行备案管理；
2. 具有相关业务的工作经验；
3. 符合本 CPS5.3.3 的要求。

如承担可信角色则需与内部人员管理要求一致。

### 5.3.8 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 审计日志程序

### 5.4.1 记录事件的类型

CMCA记录的日志信息包括但不限于以下类型：

- 1、CA密钥生命周期内的管理事件，包括密钥生成、备份、恢复、归档和销毁。

- 2、RA系统记录的证书订户身份信息。
  - 3、证书生命周期中的各项操作，包括证书申请、证书密钥更新、证书吊销等事件；
  - 4、系统、网络安全记录，包括入侵检测系统的记录、系统日常运行产生的日志文件、系统故障处理工单、系统变更工单等；
  - 5、人员访问控制记录；
  - 6、系统巡检记录。
- 上述日志信息包括记录时间、序列号、记录的实体身份、日志种类等。

### 5.4.2 处理日志的周期

CMCA 对上条中 1 类日志由密钥管理员收集并管理；2、3 类日志由数据库保存，并每天进行一次增量备份，每周进行一次全备份；4 类日志每天自动保存在备份设备上。5 类日志每季度进行一次审计；6 类日志每天进行一次检查。

### 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，离线存档至少七年。

### 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。

CMCA 有权决定是否对导致事件的实体进行通告。

## 5.4.8 脆弱性评估

CMCA 每年进行一次风险评估，内容如下：

- 1、识别可预见的内部和外部威胁，可能导致未经授权的访问、披露、误用、更改或破坏任何证书数据或证书管理过程；
- 2、评估这些威胁的可能性和潜在损害，同时考虑证书数据和证书管理过程的敏感性；和
- 3、评估 CA 为对付这些威胁而采取的政策、程序、信息系统、技术和其他

安排的充分性。

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 应保留所有与证书请求及其验证有关的文件，以及所有证书及其撤销，在基于该文件的任何证书失效后至少七年

### 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，如物理场地安全管理，存档信息异地存储，也有密码技术的保证，如存储区域密码设置，存储柜钥匙权限设置。

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。

### 5.5.7 获得和检验归档信息的程序

由两个人分别来保留归档数据的两个拷贝，并且为了确保档案信息的准确，需要对这两个拷贝进行比较。CMCA 每年会验证归档信息的完整性。

## 5.6 电子认证服务机构密钥更替

### 5.6.1 密钥更替操作

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时所采取的措施。有效期详见 6.3.2。

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。

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。

### 5.6.2 密钥更替操作管理

CMCA 建立严格的密钥更替的管理要求：

- 1、 密钥管理员提前提交密钥更替审批，经策略委员会批准后明确操作；
- 2、 密钥更替过程将全程进行记录、录像，并由第三方审计机构见证；
- 3、 密钥更替将提前 30 天通知相关方。

## 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。对于一般故障，CMCA 将在 2 小时内解决；对于紧急事件，CMCA 在

24 小时内解决；对于灾难性事件，在主运营场地出现灾难事故或不可抗力事故而不能正常运营时，CMCA 将在 48 小时内，利用备份数据和设备在数据备份中心恢复电子认证服务。

CA 应具有事件响应计划和灾难恢复计划。

CA 应编制业务连续性和灾难恢复程序，用于在发生灾难、安全损害或业务失败时通知并合理保护应用程序软件供应商、订阅者和依赖方。

CA 不需要公开披露其业务连续性计划，但应根据要求向 CA 的审计师提供其业务连续性计划和安全计划。

CA 应每年对这些程序进行测试、审查和更新。

业务连续性计划必须包含如下内容：

1. 启动计划的条件
2. 紧急程序
3. 回退过程
4. 恢复程序
5. 计划的维护计划
6. 认知和教育要求
7. 个人的责任
8. 恢复时间目标(RTO)
9. 定期测试应变计划
10. 关键业务流程中断或失败后，CA 计划及时维护或恢复 CA 的业务操作
11. 在灾难发生后的一段时间内，以及在恢复原基地或偏远地点的安全环境之前，尽可能保护其设施的程序。

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

事故和损害处理流程为:

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/或数据受到破坏时, 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，会在终止经营前九十天向给中国移动 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，按照相关法律法规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 密钥对的生成

CA 密钥对由中华人民共和国密码主管部门批准和许可的设备生成的。由于中华人民共和国对于密码产品和认证系统有严格的管理要求，因此，CMCA 在密钥的生成、管理、储存、备份和恢复时应遵循中华人民共和国相关规定进行，在此基础上，遵循 CNS 15135、ISO 19790 或 FIPS140-2 标准的相关规定，使用符合其标准的硬件设备生成和管理 CA 密钥。CA 密钥生成过程需要在独立第三方公正方见证下进行，并由其出具见证报告。CA 密钥生成日志记录在加密机设备中，将永久保存。

订户密钥对由订户自身的服务器或其它设备内置的密钥生成机制生成，中国移动 CMCA 有义务指导订户按照正确的流程生产密钥，中国移动 CMCA 拒绝弱密钥申请数字证书，并可在订户需要时提供相应的技术支持人员帮助订户生成正确的密钥。

#### 6.1.2 私钥传送给订户

私钥由订户自行生成，不需要将私钥传递给订户。OV SSL 以及 EV SSL 证书的密钥在订户自身的服务器上。

#### 6.1.3 公钥传送给证书签发机构

证书订户公钥以 PKCS #10 格式提交证书请求给 CA，应通过安全可靠的方式

式进行传输。

#### 6.1.4 CMCA 电子认证服务机构公钥传送给依赖方

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。

#### 6.1.5 密钥的长度

中国移动 CMCA 遵从国家法律法规、政府主管机构等对密钥长度的明确规定和要求，目前：

ROOT CA---RSA-4096/SHA-256

EV SSL CA---RSA-4096/SHA-256

SSL CA---RSA-4096/SHA-256

订户密钥的长度均为 RSA-4096

#### 6.1.6 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、中国移动 CMCA 数字证书签发系统支持的硬件产生。

CMCA 在采购这些设备时要求其必须具有国家密码主管部门的相应资质，并遵从国家密码主管部门发布的《证书认证系统密码及相关安全技术规范》以及其他相关规范和标准要求，如对生成的公钥参数的质量检查标准，这些设备内置的协议、算法等均已达到足够的安全等级要求等。

在使用此类硬件前，中国移动 CMCA 将对硬件进行测试，验收通过后方可投入使用，并且不定期进行公钥参数生成情况的质量检查。

#### 6.1.7 密钥使用目的

CMCA 签发的订户证书是 X509 v3 版本，包含了密钥用途扩展项。如果 CMCA 在其签发证书的密钥用途扩展项内指明了用途，证书订户必须按照该指明的用途使用密钥。

中国移动 CMCA 的私钥用于签发自身证书、子 CA 证书、订户证书和 CRL，中国移动 CMCA 的公钥用于验证私钥签名。

中国移动 CMCA 的根证书对应的私钥不能用于签署证书。

除下列情况外：

1. 自签名证书表示根 CA 本身；
2. 下级 CAs 证书和交叉证书；
3. 用于基础设施的证书(管理角色证书、内部 CA 操作设备证书);和
4. OCSP 响应验证证书。

## 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 5，N 为 3。

### 6.2.3 私钥托管

对于 CA 私钥,CMCA 无托管业务。

## 6.2.4 私钥备份

CA 的私钥由加密机产生，加密机有双机备份，并保存在防高温、防潮湿及防磁场影响的环境中，对加密机的备份操作须 3 人以上(包括 3 人)才可完成。

订户的私钥由订户产生，建议订户自行备份，并对备份的私钥采用口令或其他访问控制机制保护，防止非授权的修改或泄漏。

## 6.2.5 私钥归档

当 CMCA 的 CA 密钥对到期后，这些密钥对将被归档保存至少 10 年。归档的 CA 密钥对保存在本 CPS6.2.1 所述的硬件密码模块中，并且 CMCA 的密钥管理策略和流程都确保了归档后的 CA 密钥对不会再被用于生产系统中。当归档 CA 密钥对达到归档保存期限之后，CMCA 将按照本 CPS6.2.10 所述的方法进行安全地销毁。

CMCA 基于 PKI 理论为订户产生的加密私钥的归档参照 CA 的密钥归档方法进行归档。

CMCA 不代其他中级 CA 生归档密钥对。

## 6.2.6 私钥导入、导出密码模块

CMCA 通过硬件模块生成 CA 密钥对，部署了备份加密设备，CA 密钥对在备份传递时以离线加密方式进行。

通过硬件产生的订户私钥不能导出密码模块。其他方法产生的订户私钥在导出时应采取加密的方式进行。

CMCA 不代其他中级 CA 生归档密钥对。

## 6.2.7 私钥在密码模块的存储

私钥以密文的方式分段加密存放在通过国家密码管理部门产品鉴定的硬件



加密模块中。

CA 应当保护其密钥在至少达到 FIPS140level 3 或适当的通用标准保护配置文件或安全目标, EAL 4(或更高)的系统或设备中, 包括对已知的威胁密钥保护和其他资产的要求。

## 6.2.8 激活私钥

### ● 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。

### ● 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。

### ● 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 CMCA 私钥 5 个秘密分管者中的至少 3 人和密钥管理员同时到场，由 3 个秘密分管者输入秘密分割（激活数据）后才能激活。一旦 CA 私钥被激活，激活状态将保持到 CA 离线。

## 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。

### 6.2.11 密码模块的评估

CMCA 使用国家密码主管部门鉴定并批准使用的具有自主知识产权的高速主机加密设备, 接受其颁布的各类标准、规范、评估结果等各类要求。

## 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, 设置期限如下:

- 根证书有效期应当最长为 25 年
- 中级 CA 证书有效期最长为 20 年
- 用户证书有效期不超过 825 天

## 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。

### 6.4.3 敏感数据的其他方面

#### ● 激活数据的传输

存有 CA 私钥的加密设备和相关 IC 卡, 通常被保存在 CMCA 最安全区机房, 不能携带离开 CMCA。如在某种特殊情况下需要进行传输时（如建设灾备系统时），其传送过程需要在 CMCA 安全管理人员和密钥管理人员共同监督的情况下进行。

对于证书订户，通过网络传输用于激活私钥的口令时，需要采取加密等保护措施，以防丢失。

#### ● 激活数据的销毁

CMCA 通过对设备初始化的方式来销毁 CA 私钥的激活数据。

订户私钥的激活数据在不需要时由订户自行销毁,订户应确保他人无法通过残余信息、存储介质直接或间接地恢复激活数据。

## 6.5 计算机安全控制

### 6.5.1 具体的计算机安全技术要求

CMCA 数字证书签发系统的数据文件和设备由中国 CMCA 系统管理员维护,未经中国 CMCA 管理员授权,其它人员不能操作和控制 CMCA 系统。中国 CMCA 认证中心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 CMCA 中心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。

对于设备有一套完整的保管和维护制度:

1. 专人负责设备的领取和保管,做好设备的领用、进出库和报废登记。
2. 对设备定期进行检查、清洁和保养维护。
3. 制定设备维修计划,建立满足正常运转最低要求的易损坏备件库。
4. 对设备进行维修时,必须记录维修的对象、故障原因、排除方法、主要
5. 维修过程及与维修有关的情况等。
6. 设备维修时,必须有派专人在场监督。
7. 唯一的设备密码。

并且每一个使用 CMCA 系统的人员必须使用唯一的数字证书,人员配置的访问限制为执行工作职责要求的最小权限,满足双因素认证。

CA 对所有能够直接导致证书颁发的账户实施多因素认证。

### 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

CMCA 签发的证书均符合 X.509 V3 证书格式。均按照 RFC5280 设置, 符合 CA/Browser 的当前版本要求。证书的最基本字段与内容见下表。

CMCA GLOBAL TRUST ROOT CA

证书域	域值
版本	V3
序列号	包含 24 位的随机数
签名算法	SHA256RSA
颁发者	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN
有效期起止日	证书有效期起始时间
有效期终止日	证书有效期终止时间
主题	证书的主题 DN, 见 CSP7.1.4
公钥	RSA (4096)
基本限制	Subject Type=CA Path Length Constraint=None
密钥用法	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

CMCA SSL CA

证书域	域值
版本	V3
序列号	包含 24 位的随机数
签名算法	SHA256RSA
颁发者	CN = CMCA GLOBAL TRUST ROOT CA



	O = Aspire Technologies C = CN
有效期起止日	证书有效期起始时间
有效期终止日	证书有效期终止时间
主题	证书的主题 DN, 见 CSP7.1.4
公钥	RSA (4096)
颁发机构访问信息	[1]Authority Info Access Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2) Alternative Name:  URL=https://mpus.cmca.net:8080/files/downloadcenter/CMCA GLOBALTRUSTROOTCA.cer [2]Authority Info Access Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=https://mpus.cmca.net:8080/ocsp
基本限制	Subject Type=CA Path Length Constraint=None
证书策略	[1]Certificate Policy: Policy Identifier=所有颁发策略 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://mpus.cmca.net:8080/files/downloadcenter/cps.doc
CRL 发布点	该发布点包含了一个 URL, 用于获得 CRL 文件。
密钥用法	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

### CMCA EV SSL CA

证书域	域值
版本	V3
序列号	包含 24 位的随机数
签名算法	SHA256RSA

颁发者	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN
有效期起止日	证书有效期起始时间
有效期终止日	证书有效期终止时间
主题	证书的主题 DN, 见 CSP7.1.4
公钥	RSA (4096)
颁发机构访问信息	[1]Authority Info Access Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2) Alternative Name:  URL=https://mpus.cmca.net:8080/files/downloadcenter/CMCA GLOBALTRUSTROOTCA.cer [2]Authority Info Access Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=https://mpus.cmca.net:8080/ocsp
基本限制	Subject Type=CA Path Length Constraint=None
证书策略	[1]Certificate Policy: Policy Identifier=所有颁发策略 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://mpus.cmca.net:8080/files/downloadcenter/cps.doc
CRL 发布点	该发布点包含了一个 URL, 用于获得 CRL 文件。
密钥用法	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

### 订户证书 (EV)

证书域	域值
版本	V3
序列号	包含 24 位的随机数

签名算法	SHA256RSA
颁发者	CN = CMCA EV SSL CA O = Aspire Technologies C = CN
有效期起止日	证书有效期起始时间
有效期终止日	证书有效期终止时间
主题	证书的主题 DN, 见 CSP7.1.4
公钥	RSA (4096)
颁发机构访问信息	<p>[1]Authority Info Access Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2) Alternative Name:  URL=https://mpus.cmca.net:8080/files/downloadcenter/CMCAEVSSLC A.cer</p> <p>[2]Authority Info Access Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=https://mpus.cmca.net:8080/ocsp</p>
证书策略	<p>[1]Certificate Policy: Policy Identifier=2.23.140.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://mpus.cmca.net:8080/files/downloadcenter/cps.doc</p>
CRL 发布点	该发布点包含了一个 URL, 用于获得 CRL 文件。
密钥用法	Digital Signature, Key Encipherment (a0)
增强密钥用法	客户端身份验证 (1.3.6.1.5.5.7.3.2) 服务器身份验证 (1.3.6.1.5.5.7.3.1)
主题备用名	域名

### 订户证书 (OV)

证书域	域值
版本	V3
序列号	包含 24 位的随机数

签名算法	SHA256RSA
颁发者	CN = CMCA SSL CA O = Aspire Technologies C = CN
有效期起止日	证书有效期起始时间
有效期终止日	证书有效期终止时间
主题	证书的主题 DN, 见 CSP7.1.4
公钥	RSA (4096)
颁发机构访问信息	<p>[1]Authority Info Access Access Method=证书颁发机构颁发者 (1.3.6.1.5.5.7.48.2) Alternative Name:  URL=https://mpus.cmca.net:8080/files/downloadcenter/CMCASSLCA.cer</p> <p>[2]Authority Info Access Access Method=联机证书状态协议 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=https://mpus.cmca.net:8080/ocsp</p>
证书策略	<p>[1]Certificate Policy: Policy Identifier=2.23.140.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://mpus.cmca.net:8080/files/downloadcenter/cps.doc</p>
CRL 发布点	该发布点包含了一个 URL, 用于获得 CRL 文件。
密钥用法	Digital Signature, Key Encipherment (a0)
增强密钥用法	客户端身份验证 (1.3.6.1.5.5.7.3.2) 服务器身份验证 (1.3.6.1.5.5.7.3.1)
主题备用名	域名

## 7.1.1 证书版本号

X.509 V3。

## 7.1.2 证书扩展项

CMCA 签发的证书，其证书扩展项遵循 IETF RFC 5280 标准要求。

。

### 7.1.2.1 根证书扩展项目

#### 1、 密钥用法 (Key Usage)

按照 RFC5280 进行填充，内容为 Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)，该项的 criticality 域设置为 true。

#### 2、 基本约束 (Basic Constraints)

Path Length Constraint=None，该项的 criticality 域设置为 true。

#### 3、 颁发者机构密钥标识符 (Authority Key Identifier)

颁发者机构密钥标识符由根 CA 证书公钥的 160 位 SHA1 散列组成。该项的 criticality 域设置为 false。

#### 4、 主体密钥标识符 (Subject Key Identifier)

主体密钥标识符由根 CA 证书公钥的 160 位 SHA1 散列组成。该项的 criticality 域设置为 false。

### 7.1.2.2 中级证书扩展项

#### 1、 密钥用法 (Key Usage)

按照 RFC5280 进行填充，内容为 Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)，该项的 criticality 域设置为 true。

#### 2、 证书策略 (Certificate Policies Extension)

按照 RFC5280 进行填充。该项的 criticality 域设置为 false。

### 3、基本约束 (Basic Constraints)

Path Length Constraint=None, 该项的 criticality 域设置为 true。

### 4、CRL 发布点 (CRL Distribution Points)

该发布点包含了一个 URL, URL 地址为

https://mpus.cmca.net:8080/crl/crl1.crl 用于获得 CRL 文件, 该项的 criticality 域设置为 false。

### 5、颁发者机构密钥标识符 (Authority Key Identifier)

颁发者机构密钥标识符由根 CA 证书公钥的 160 位 SHA1 散列组成。该项的 criticality 域设置为 false。

### 6、主体密钥标识符 (Subject Key Identifier)

主体密钥标识符由中级 CA 证书公钥的 160 位 SHA1 散列组成。该项的 criticality 域设置为 false。

### 7、颁发者机构访问 (Authority Info Access)

颁发者机构访问为联机证书状态协议, 该项的 criticality 域设置为 false。

## 7.1.2.3 订户证书扩展项

#### 1、密钥用法 (Key Usage)

按照 RFC5280 进行填充, 内容为 Digital Signature, Key Encipherment (a0), 该项的 criticality 域设置为 true。

#### 2、证书策略 (Certificate Policies Extension)

按照 RFC5280 进行填充。该项的 criticality 域设置为 false。

#### 3、扩展密钥用法 (Extended Key Usage)

如果有将按照 RFC5280 进行填充, 内容为客户端身份验证 (1.3.6.1.5.5.7.3.2), 服务器身份验证 (1.3.6.1.5.5.7.3.1)。该项的 criticality 域设置为 false。

#### 4、CRL 发布点 (CRL Distribution Points)

该发布点包含了一个 URL, 用于获得 CRL 文件, 该项的 criticality 域设置为 false。

### 5、颁发者机构密钥标识符 (Authority Key Identifier)

颁发者机构密钥标识符由中级CA证书公钥的160位SHA1散列组成。该项的 criticality域设置为false。

### 6、主题密钥标识符 (Subject Key Identifier)

主题密钥标识符标识了被认证的公钥，可用于区分同一主体使用的不同密钥（如证书密钥更新时）。其值从公钥中或者生成唯一值的方法导出。该项的 criticality域设置为false。

### 7、颁发者机构访问 (Authority Info Access)

颁发者机构访问为联机证书状态协议，该项的 criticality 域设置为 false。

### 8、使用者备用名称 (Subject Alternative Name)

按照 RFC5280 进行填充，该项的 criticality 域设置为 false。

## 7.1.3 算法对象标识符

中国移动 CMCA 签发的证书按照 RFC 5280 标准，用 SHA256 算法签名。

## 7.1.4 名称形式

CMCA 签发的证书（包括根证书、中间证书以及订户证书）的 DN 都采用 X.500 (Distinguished Name; DN) 命名方式，遵循 RFC5280 相关规定。

### 7.1.4.1 证书颁发者

#### ➤ OV SSL 证书

CN = CMCA OV SSL CA

O = Aspire Technologies

C = CN

#### ➤ EV SSL 证书

CN = CMCA EV SSL CA

O = Aspire Technologies

C = CN

#### ➤ CMCA EV SSL CA 中级证书



CN = CMCA GLOBAL TRUST ROOT CA

O = Aspire Technologies

C = CN

➤ CMCA SSL CA 中级证书

CN = CMCA GLOBAL TRUST ROOT CA

O = Aspire Technologies

C = CN

➤ CMCA GLOBAL TRUST ROOT CA 根证书

CN = CMCA GLOBAL TRUST ROOT CA

O = Aspire Technologies

C = CN

#### 7.1.4.2 证书主题

CMCA 签发证书的甄别名符合 X.500 关于甄别名的规定。CMCA 保证签发的每一个证书的甄别名都是唯一的。

DN 项中包含的国家、省市级名称必须使用权威部门发布的标准名称。(如 SO country code) 。

##### 7.1.4.%1 订户证书 DN 要求

- 1、CN 部分：订户的真实域名；
- 2、OU 部分：可以表示实体的部门名称及经客户确认的有效信息；
- 3、O 部分：可以表示实体的真实名称；
- 4、L 部分：用于表示注册地址或运营地址所在城市或同等级别行政区域；
- 5、S 部分：用于表示注册地址或运营地址所在省或同等级别行政区域；
- 6、C 部分：用于标识营业地址所在国家或地区，全部大写，如中国订户标识为 C=CN。

订户在申请证书时应参照此要求生成证书签名请求文件（CSR，Certificate Signature Request），经 CMCA 审核通过后由 CMCA 签发证书。

#### 7.1.4.2 CMCA EV SSL CA

- 1、CN 部分：CMCA EV SSL CA;
- 2、O 部分：Aspire Technologies;
- 3、C 部分：CN。

#### 7.1.4.3 CMCA SSL CA

- 1、CN 部分：CMCA SSL CA;
- 2、O 部分：Aspire Technologies;
- 3、C 部分：CN。

#### 7.1.4.4 CMCA GLOBAL TRUST ROOT CA

- 1、CN 部分：CMCA GLOBAL TRUST ROOT CA;
- 2、O 部分：Aspire Technologies;
- 3、C 部分：CN。

### 7.1.5 名称限制

CMCA 全球信任体系下签发的证书，其实体名称不允许为匿名或者伪名，必须是有明确含义的识别名称，使用英文名称时应能正确表达实体名称。

### 7.1.6 证书策略对象标识符

CA 中级证书的证书策略扩展项中，certificatePolicies:policyIdentifier 设置为 anyPolicy;

订户证书策略对象标识符如下：

OV SSL 证书对应的证书策略对象标识号符 (OID) 为 2.23.140.1.2.2。

EV SSL 证书对应的证书策略对象标识号符 (OID) 为 2.23.140.1.2.2。

CMCA 签发的证书应包含策略标识符。证书策略标识符包含一个证书策略对象标识符 OID 和 URL 地址。订户证书的证书策略对象标识符见 1.2, 中级证书的证书策略对象标识符是所有策略, 根证书没有证书策略对象标识符。订户证书、中级证书策略表述 URL 为

<https://mpus.cmca.net:8080/files/downloadcenter/cps.doc>

证书标识符符合CA/浏览器论坛 (CA/Browsr Forum) 通过 [www.cabforum.org](http://www.cabforum.org) 发布的指南7.1.6部分要求。

## 7.1.7 策略限制扩展项的用法

未使用本扩展域。

## 7.1.8 策略限定符的语法和语义

未使用本扩展域。

## 7.1.9 关键证书策略扩展项的处理规则

未使用本扩展域。

## 7.2 证书吊销列表

CMCA 定期签发 CRL (证书废除列表), 供订户查询使用。具体参见 SGP.22 。

### 7.2.1 版本号

X.509: V2。

## 7.2.2 CRL 和 CRL 条目扩展项

CRL 符合 RFC5280 要求。列表包含最基本的字段和内容中指定下面的表:

字段	内容
Version	参考 7.2.1 章节
Signature Algorithm	用于对 CRL 进行签名的算法。参考 RFC3279
Issure	签发 CRL 的实体, CRL 的颁发者。
Effective Date	CRL 文件的发布时间
Next Update	CRL 的下一步发布时间。CRL 的发布频率参考 4.9.7.
Revoked Certificates	插销的证书清单。包括证书序列号以及撤销日期, 撤销原因。

CRL 基本字段

中国移动 CMCA 每隔 24 小时自动发布最新的 CRL。

## 7.3 在线证书状态查询协议

CMCA 为证书用户提供 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。采用 RFC 2560 OCSP 协议。

### 7.3.1 版本号

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。

## 7.3.2 OCSP 扩展项

与 RFC2560 一致。

# 8 认证机构审计和其他评估

## 8.1 审计的频率或情形

CMCA在如下情形中进行评估:

- 1、根据《中华人民共和国电子签名法》、《电子认证服务管理办法》《电子认证服务密码管理办法》规定，接受主管部门的评估和检查。
- 2、接受外部审计机构的定期评估。
- 3、接受第三方审计公司的Webtrust审计。

评估的频率为:

- 1、年度评估: 接受主管部门对CMCA进行的检查，通常为年度检查，具体已主管部门要求为主;
- 2、定期评估: 按照国际及国内相关标准要求接受外部审计机构的定期评估。
- 4、CMCA将每年进行Webtrust审计，且审计报告发布日期不得晚于审计期间结束后三个月。

## 8.2 审计者的资质

若需邀请外部审计机构对CMCA进行评估，CMCA将选择熟悉IT运营管理、具有多年审计经验的审计机构对CMCA的运营管理进行一致性审计。在进行审计前，审计机构必须熟悉公钥基础设施技术及相关的法律法规、标准规范要求。

对于外部审计师的要求如下:

从业者必须是具有提供与信息科技、信息安全、PKI和系统审计有关的第三方认证服务资质的独立会计师事务所; 从业者在提供服务时，其EV证书WebTrust审核服务资质必须是有效的; 从业者必须是AICPA或其他具有明确成员

资质标准的协会成员。

## 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

审计者与中国移动 CMCA 应无任何业务、财务往来或其它足以影响评估客观性的利害关系。

## 8.4 审计内容

对中国移动 CMCA 的审计包括但不限于以下内容：

- 1、CA 物理环境和控制
- 2、密钥管理操作
- 3、基础 CA 控制
- 4、证书生命周期管理
- 5、CA 业务规则

## 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

当CMCA接受行业主管部门的检查或评估后，行业主管部门会向公众发布对CMCA的检查或评估结果。

当CMCA接受外部审计机构的审计后，CMCA会在公司网站上公布外部审计结果。

当 CMCA 进行内部审计后，审计结果将只在公司内部进行传达。

## 8.7 其他

CMCA 在证书签发期间为严格控制服务质量以及保证对 CP、CPS 及 BR 准则的符合性应至少每季度要进行一次自我审计，随机抽取百分之三（如小于一则抽取一份样本）的样本进行评估。

## 9 法律责任和其他业务条款

### 9.1 费用

#### 9.1.1 证书签发和更新费用

根据市场和管理部门的规定，CMCA将收取合理的费用，并在订户向CMCA订购证书时，提前告知证书的签发与更新费用。

#### 9.1.2 证书查询费用

CMCA 暂不收取此项收费，但保留对此项服务收费的权利。

#### 9.1.3 证书吊销或状态信息的查询费用

CMCA 暂不收取此项收费，但保留对此项服务收费的权利。

#### 9.1.4 其他服务费用

CMCA 保留收取其他服务费用的权利。



### 9.1.5 退款策略

除非CMCA违背了本CPS所规定的责任与义务，订户可以要求退款。否则，CMCA对订户收取的费用均不退还。

订户应当提供符合CMCA要求的完整、真实、准确的证书申请信息，否则CMCA对此造成的损失和后果不承担任何责任。

## 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 其他资产

CMCA 确保具有足够的财务实力来维持其正常经营并保证相应义务的履行，并合理地承担对订户及对依赖方的责任。

此要求对证书订户同样适用。

### 9.2.3 对最终实体的保险或担保

如果 CMCA 根据本 CPS 或任何法律规定，以及司法判定须承担赔偿责任和/或补偿责任的，CMCA 将按照相关法律法规的规定、仲裁机构的裁定或法院的判决承担相应的赔偿责任。

## 9.3 业务信息保密

### 9.3.1 保密信息范围

1、CMCA与订户之间的协议、资料中未公开的内容等属于保密信息。除非法律明文规定或政府、执法机关等的要求，CMCA承诺不对外公布或透露订户证书信息以外的任何其它隐私信息。

2、订户私钥属于机密信息，订户应当根据本CPS的规定妥善保管，如因订户自己泄漏私钥造成的损失，订户应自行承担。

### 9.3.2 不属于保密的信息

- 1、CA系统签发的证书信息和CRL中的信息。
- 2、在提供方披露数据和信息之前，已被接受方所持有的数据和信息。
- 3、在提供方披露数据和信息时或在披露数据和信息之后，非由于接受方的原因而被披露的信息。
- 4、经公开或通过其他途径成为公众领域的一部分数据和信息。
- 5、有权披露的第三方披露给接受方的数据和信息。
- 6、其他可以通过公共、公开渠道获得的信息。

### 9.3.3 保护保密信息的责任

CMCA 有各种严格的管理制度、流程和技术手段来保护机密信息，包括但

不限于商业机密、客户信息等。CMCA 的每个员工都要接受信息保密方面的培训。

## 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。

CMCA 尊重所有订户和他们的隐私，个人隐私信息保密方案遵守现行法律明已经同意接受 CMCA 的隐私保护制度。

### 9.4.2 作为隐私处理的信息

CMCA 在管理和使用订户提供的相关信息时，除了证书中已经包括的信息以及证书状态信息外，该订户的基本信息将被视为隐私处理，这些信息将只能由 CMCA 使用，非经订户同意或有关法律法规、公共权力部门根据合法的程序要求，CMCA 不会任意公开。同时 CMCA 不会对外提供证书检索服务。

### 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

CMCA、注册机构、订户、依赖方等机构或个人都有义务按照本CPS的规定，承担相应的隐私保护责任。在法律法规或公共权力部门通过合法程序要求下，CMCA可以向特定的对象公布隐私信息，CMCA无需承担由此造成的任何责任。

### 9.4.5 使用隐私信息的告知与同意

1、订户同意，CMCA在业务范围内并按照本CPS规定的隐私保护政策使用所获得的任何订户信息，无论是否涉及到隐私，CMCA均可以不用告知订户。

2、订户同意，在任何法律法规或公共权力部门要求下，CMCA向特定对象披露隐私信息时，CMCA均可以不用告知订户。

### 9.4.6 依法律或行政程序的信息披露

除非符合下列条件，CMCA不会将订户的保密信息提供给其他个人或第三方机构：

1、司法、行政部门或其他法律法规授权的部门依据政府法律法规、规章、决定、命令等的规定通过合法授权提出的申请。

2、订户采用书面形式的信息披露授权。

3、本CPS规定的其他可以披露的情形。

### 9.4.7 其他信息披露情形

CMCA、订户、注册机构、依赖方等机构或个人都有义务按照本CPS的规定，承担相应的保护隐私责任。在法律法规或公共权力部门通过合法程序或订户书面申请授权要求下，CMCA可以向特定的对象公布隐私信息，CMCA无需承担由此造成的任何责任。

## 9.5 知识产权

CMCA享有并保留对证书以及CMCA提供的全部软件、资料、数据等的著作权、专利申请权等全部知识产权；CMCA制订并发布的CPS、CP、技术支持手册、发布的证书和CRL等的所有权和知识产权均归属于CMCA。

## 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
- 中国移动 CMCA 向证书受益人（订户、应用软件供应方、依赖方）声明及保证，在证书有效期内，CMCA 在签发及管理证书时，已遵守 BR 规定，以及 CMCA 的 CP 与 CPS。
- 中国移动 CMCA 证书担保在证书业务过程中，对以下信息 进行完整准确的验证，经过验证通过后，才对执行相关证书操作：
  - 1.使用域名或 IP 地址的权利
  - 2.证书授权
  - 3.信息的准确性
  - 4.没有误导信息
  - 5.申请人身份
  - 6.用户协议
  - 7.状态
  - 8.撤销，

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

在签发证书之前，为了 CA 和证书受益人的明确利益，证书订户必须提交纸质的签字和盖章的《CMCA 数字证书申请表》。所有的证书订户一旦提交该项材料，即默认用户同意《中国移动 CMCA 数字证书订户协议》中的所有条款，用户一旦违反订户协议中的条款，将承担因违反条款所带来的后果与责任，包括相应的法律责任。

证书申请人为 CA 和证书受益人作出承诺和保证。

- 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，严格保护证书的密钥；
- 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，证书订户对其提交的所有证书申请材料真实性负责，供中国移动 CMCA 或受理点检查和核实；
- 证书签发后，证书订户通过证书申请表上的邮箱接受 CMCA 签发的证书；
- 证书订户保证所申请的证书在合理合法范围内使用，如违规使用，证书订户承担因此带来的一切问题与责任。
- 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。
- 如证书订户需要终止使用证书，应及时向 CA 中心提出申请。

## 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

如果 CMCA 根据本 CPS 或任何法律规定，以及司法判定须承担赔偿责任和/或补偿责任的，CMCA 将按照相关法律法规的规定、仲裁机构的裁定或法院的判决承担相应的赔偿责任。

## 9.9 赔偿

1、除非有另外的规定或约定，对于非因本CPS项下的认证服务而导致的任何损失，CMCA不向订户和/或依赖方承担任何赔偿和/或补偿责任。

2、订户或依赖方进行的民事活动因CMCA提供的认证服务而遭受的损失，CMCA将依据本CPS的相关条款给予相应的赔偿。但无论如何，如果CMCA能够证明其提供的服务是按照《电子签名法》、《电子认证服务管理办法》、CMCA向主管部门备案的CPS实施的，则视为CMCA不具有任何过错，CMCA将不对订户或依赖方承担任何赔偿或补偿责任。

3、无论本CPS是否有相反或不同规定，就以下损失或损害，CMCA不承担任何赔偿和/或补偿责任：

(1) 订户和/或依赖方的任何间接损失、直接或间接的利润或收入损失、信誉或商誉损害、任何商机或契机损失、失去项目、以及失去或无法使用任何数据、无法使用任何设备、无法使用任何软件；

(2) 由上述第 (1) 项所述的损失相应生成或附带引起的损失或损害；

(3) 非CMCA的行为而导致的损失；

(4) 因不可抗力而导致的损失，如罢工、战争、灾害、恶意代码病毒等。

4、无论本CPS是否有相反或不同规定，如果CMCA根据本CPS或任何法律规定，以及司法判定须承担赔偿责任和/或补偿责任的，CMCA 将按照相关法律法规的规定、仲裁机构的裁定或法院的判决承担相应的赔偿责任。

## 9.10 有效期限与终止

### 9.10.1 有效期限

本 CPS 自发布之日起正式生效，上一版本的 CPS 同时失效；本 CPS 在下一版本 CPS 生效之日或在 CMCA 终止电子认证服务时失效。

### 9.10.2 终止

CMCA 终止电子认证服务时，本 CPS 终止。

### 9.10.3 效力的终止与保留

本 CPS 终止后，其效力将同时终止，CPS 中的内容将视为无效使用，但对终止之日前发生的法律事实，本 CPS 中对各方责任的规定及责任免除仍然适用。

## 9.11 对参与者的个别通告与沟通

参与者如需要进一步了解任何本 CPS 中提及的服务、规范、操作等信息，可

以通过网站或者邮件联系 CMCA。

联系网站: [www.cmca.net](http://www.cmca.net)

联系邮箱: [cmca@aspirecn.com](mailto:cmca@aspirecn.com)

## 9.12 修订

### 9.12.1 修订程序

修订程序与本CPS1.5.4“CPS批准程序”相同。

### 9.12.2 通知机制和期限

修订后的 CPS 经批准后将立即在 CMCA 的网站 [www.cmca.net](http://www.cmca.net) 上发布。

### 9.12.3 必须修改业务规则的情形

CMCA 必须对本 CPS 进行修改的情形包括: CPS 中相关内容与管辖法律的不一致, 国家监管部门对本机构认证业务有明确的更改或调整要求等。

## 9.13 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)有限公司注册地所在人民法院管辖。

## 9.14 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。

## 9.15 适用法律的符合性

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。

## 9.16 一般条款

### 9.16.1 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。

### 9.16.2 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偿证券）中国移动 CMCA 的 CPS 详述的权利和义务。

### 9.16.3 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。

#### 9.16.4 强制执行

CMCA 声明，证书订户、依赖方等必须执行 CMCA 的 CPS 中的所有规定。若证书订户、依赖方等实体未执行 CMCA 的 CPS 中某项规定，不被认为该实体将来不执行该项或其他规定。

#### 9.16.5 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。

#### 9.17 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。