



中国移动证书信任体系扩展证书策略

<版本：V0.1>

生效日期：2010 年 9 月 10 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	2010.9.10	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 (CA)	2
1.3.2 注册机构 (RA)	3
1.3.3 受理点 (LRA)	3
1.3.4 订户.....	3
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 证书类型和应用范围.....	4
1.4.2 限制的证书应用.....	6
1.4.3 受禁的证书应用.....	7
1.5 策略管理.....	7
1.5.1 策略文档管理机构.....	7
1.5.2 联系人.....	7
1.5.3 决定 CP 符合策略的机构.....	8
1.5.4 CP 批准程序.....	8
1.6 定义和缩写.....	8
2. 信息发布与信息管理.....	9
2.1 信息库.....	9
2.2 信息发布.....	9
2.3 发布的时间或频率.....	10
2.4 信息库访问控制.....	10
3. 身份标识与鉴别.....	11
3.1 命名.....	11
3.1.1 名称类型.....	11
3.1.2 对名称有意义的要求.....	11
3.1.3 订户的匿名或伪名.....	11
3.2 初始身份确认.....	12
3.2.1 证明拥有私钥的方法.....	12
3.2.2 手机号码的鉴别.....	12
3.2.3 手机用户个人身份的鉴别.....	12
3.2.4 移动终端设备身份的鉴别.....	13
3.2.5 终端应用个人开发者身份的鉴别.....	13
3.2.6 终端应用企业开发者身份的鉴别.....	错误! 未定义书签。

3.3	更新请求的标识与鉴别.....	14
3.3.1	常规更新的标识与鉴别.....	15
3.3.2	吊销后更新的标识与鉴别.....	15
3.4	吊销请求的标识与鉴别.....	15
4.	证书生命周期操作要求.....	16
4.1	证书申请.....	16
4.1.1	证书申请实体.....	16
4.1.2	注册过程与责任.....	16
4.2	证书审核.....	16
4.2.1	执行识别与鉴别功能.....	16
4.2.2	证书申请批准和拒绝.....	16
4.2.3	处理证书申请的时间.....	16
4.3	证书签发.....	17
4.3.1	签发证书.....	17
4.3.2	拒绝签发证书.....	17
4.4	证书接受.....	17
4.4.1	证书接受.....	17
4.4.2	证书的发布.....	17
4.5	密钥和证书的使用.....	18
4.5.1	订户私钥和证书的使用.....	18
4.5.2	依赖方公钥和证书的使用.....	18
4.6	证书更新.....	18
4.6.1	证书更新的原因.....	18
4.6.2	请求证书更新的实体.....	19
4.6.3	证书更新流程.....	19
4.6.4	对更新证书的发布.....	19
4.7	证书密钥更新.....	19
4.7.1	密钥更新的原因.....	19
4.7.2	请求密钥更新的实体.....	19
4.7.3	密钥更新的流程.....	20
4.7.4	对更新证书的发布.....	20
4.8	证书变更.....	20
4.8.1	证书变更的原因.....	20
4.8.2	请求证书变更的实体.....	20
4.8.3	证书变更的流程.....	20
4.8.4	对变更后新证书的发布.....	20
4.9	证书吊销.....	21
4.9.1	证书吊销的原因.....	21
4.9.2	请求证书吊销的实体.....	21
4.9.3	吊销请求的流程.....	21
4.9.4	吊销请求宽限期.....	22
4.9.5	电子认证服务机构处理吊销请求的时限.....	22
4.9.6	依赖方检查证书吊销的要求.....	22

4.9.7	CRL 发布频率.....	22
4.9.8	在线状态查询要求.....	23
4.10	证书挂起.....	23
4.10.1	证书挂起的原因.....	23
4.10.2	请求证书挂起的实体.....	23
4.10.3	挂起请求的流程.....	23
4.10.4	挂起的期限限制.....	24
4.11	证书解挂.....	24
4.11.1	证书解挂的原因.....	24
4.11.2	请求证书解挂的实体.....	24
4.11.3	证书解挂的流程.....	24
4.12	密钥恢复.....	25
4.12.1	密钥恢复的原因.....	25
4.12.2	请求密钥恢复的实体.....	25
4.12.3	密钥恢复的流程.....	25
4.13	证书状态服务.....	25
4.14	CA 服务终止.....	25
4.15	密钥生成、备份与恢复.....	26
5.	认证机构设施、管理和操作安全控制.....	26
5.1	物理安全控制.....	26
5.1.1	物理场地安全.....	26
5.1.2	物理访问.....	27
5.1.3	电力与空调.....	27
5.1.4	水患防治.....	27
5.1.5	火灾防护.....	27
5.1.6	介质存储.....	27
5.1.7	废物处理.....	27
5.1.8	异地备份.....	28
5.2	流程安全控制.....	28
5.2.1	可信角色.....	28
5.2.2	每项任务需要的人数.....	30
5.2.3	安全令牌控制.....	30
5.2.4	职责分割原则.....	30
5.3	人员控制.....	30
5.3.1	资格、经历和无过失要求.....	30
5.3.2	背景审查程序.....	31
5.3.3	培训要求.....	31
5.3.4	再培训周期和要求.....	31
5.3.5	岗位分离和轮换.....	31
5.3.6	未授权行为的处罚.....	31
5.3.7	提供给员工的文档.....	32
5.4	安全审计.....	32
5.4.1	记录事件的类型.....	32

5.4.2	处理日志的周期.....	33
5.4.3	审计日志的保存期限.....	33
5.4.4	审计日志的保护.....	34
5.4.5	审计日志备份程序.....	34
5.4.6	审计收集系统.....	34
5.4.7	对导致事件实体的处理.....	34
5.4.8	脆弱性评估.....	34
5.5	记录归档.....	34
5.5.1	归档记录的类型.....	34
5.5.2	归档记录的保存期限.....	35
5.5.3	归档文件的保护.....	35
5.5.4	归档文件的备份.....	35
5.5.5	记录时间戳要求.....	35
5.5.6	归档收集系统.....	35
5.6	密钥更替.....	35
5.7	损害与灾难恢复.....	36
5.8	电子认证服务机构或注册机构的业务终止.....	36
5.8.1	CA 终止原因.....	36
5.8.2	终止通知.....	36
5.8.3	终止归档.....	36
5.8.4	RA 的终止.....	36
6.	认证系统技术安全控制.....	37
6.1	密钥对的生成和安装.....	37
6.1.1	CA 密钥对的产生.....	37
6.1.2	订户密钥对的生成.....	37
6.1.3	私钥传送.....	37
6.1.4	公钥传送.....	38
6.1.5	电子认证服务机构公钥传送.....	38
6.1.6	密钥的长度.....	38
6.1.7	公钥参数的生成.....	38
6.1.8	密钥用途.....	38
6.2	私钥保护和密码模块工程控制.....	39
6.2.1	密码模块的标准和控制.....	39
6.2.2	私钥多人控制.....	39
6.2.3	私钥托管.....	39
6.2.4	私钥备份.....	39
6.2.5	私钥归档.....	40
6.2.6	私钥导入、导出密码模块.....	40
6.2.7	私钥在密码模块的存储.....	40
6.2.8	激活私钥.....	40
6.2.9	解除私钥激活状态（应根据证书类别进行拆分）.....	41
6.2.10	销毁私钥.....	41
6.3	密钥对管理的其他方面.....	41

6.3.1	公钥归档.....	41
6.3.2	证书操作期和密钥对使用期.....	41
6.4	敏感数据.....	42
6.4.1	敏感数据的产生.....	42
6.4.2	敏感数据的保护.....	42
6.5	计算机安全控制.....	42
6.5.1	计算机安全技术要求.....	42
6.5.2	计算机安全评估.....	43
6.6	网络的安全控制.....	43
6.7	时间戳.....	43
7.	证书、证书吊销列表和在线证书状态协议.....	44
7.1	证书.....	44
7.1.1	版本号.....	44
7.1.2	证书标准项.....	44
7.1.3	证书扩展项.....	45
7.1.4	密钥算法对象标识符.....	47
7.1.5	名称格式.....	47
7.2	证书吊销列表.....	47
7.2.1	版本号.....	47
7.2.2	CRL 和 CRL 条目扩展项.....	47
7.3	在线证书状态查询协议.....	48
8	认证机构审计和其他评估	49
8.1	审计的频率或情形	49
8.1.1	认证机构的审计.....	49
8.1.2	认证机构对关联单位的审计.....	49
8.2	审计者的资质	49
8.3	审计者与认证机构的关系	50
8.3.1	审计者与认证机构的关系.....	50
8.3.2	审计报告与认证机构 的关系.....	50
8.4	审计内容	50
8.5	对问题与不足采取的措施	50
8.6	评估结果的传达与发布	51
9	法律责任和其他业务条款	51
9.1	费用	51
9.1.1	证书费用.....	51
9.1.2	退款策略.....	51
9.2	财务责任	51
9.2.1	保险范围.....	52
9.2.2	对最终实体的保险或担保.....	52
9.3	业务信息保密	52
9.3.1	保密信息范围.....	52

9.3.2 不属于保密的信息.....	52
9.3.3 对业务信息保密的责任.....	53
9.4 个人隐私保密	53
9.4.1 隐私保密方案.....	53
9.4.2 作为隐私处理的信息.....	53
9.4.3 不被视为隐私的信息.....	53
9.4.4 保护隐私的责任.....	53
9.4.5 依法律或行政程序的信息披露.....	54
9.4.6 其他信息披露情形.....	54
9.5 知识产权	54
9.6 陈述与担保	54
9.6.1 电子认证服务机构的陈述与担保.....	54
9.6.2 注册机构的陈述与担保.....	55
9.6.3 订户的陈述与担保.....	55
9.6.4 依赖方的陈述与担保.....	56
9.6.5 其他参与者的陈述与担保.....	56
9.7 担保免责	56
9.8 有限责任	57
9.9 赔偿	57
9.9.1 赔偿条件.....	57
9.9.2 赔偿限制.....	59
9.9.3 其他机构赔偿.....	59
9.10 有效期限与终止.....	59
9.11 修订	59
9.12 争议处理	60
9.13 管辖法律	60
9.14 适用的法律.....	60
9.15 一般条款.....	60
9.15.1 完整协议.....	60
9.15.2 转让	60
9.15.3 分割性	60
9.15.4 不可抗力.....	61
9.16 其他条款.....	61

1. 概括性描述

1.1 概述

中国移动证书信任体系（China Mobile Certificate Trust Network，简称 CMCTN）是一个以中国移动用户为主的公钥基础设施（Public Key Infrastructure，PKI），它向用户提供的数字证书可适合于广大的、对通信和信息安全方面有各种各样的需求的公众用户。

CMCTN 的证书分为两个信任等级，分别为基线证书（可称为基础标准证书）和扩展证书（可称为移动特色证书），根据不同等级证书的安全策略要求和服务能力，CMCTN 分别制定了不同等级的（Certificate Policy，CP），即中国移动证书信任体系基线证书策略和中国移动证书信任体系扩展证书策略。

本文档中国移动证书信任体系扩展证书策略。本证书策略根据国家相关法律法规的要求，详细阐述了 CMCTN 的认证机构在提供相关可信服务时在商务、法律和技术方面应遵循的规范，以及电子认证服务参与各方所承担的责任与义务，CMCTN 的认证机构及其授权注册机构（RA）和业务受理点（LRA）必须遵循本证书策略中的各项规范。CMCTN 体系内的实体，包括 CMCTN 数字证书订户，在参与电子认证服务前有义务了解本证书策略所规定的条款，承担相应的责任和义务，并据此监督 CMCTN 的认证机构及其授权注册机构和业务受理点的规范运营。

证书策略是管辖中国移动证书信任体系的主要策略说明。根据本证书策略制定的电子认证业务规则（CPS），不能出现与本证书策略内容冲突的条款。

中国移动 CA 中心（China Mobile Certificate Authority，简称 CMCA）的安全认证策略管理委员会（Policy Management Authority，PMA）负责此 CP 的修改、更新及评述整理工作。PMA 还负责检查 CP 要求的遵守情况。

本 CP 的结构符合“互联网 X.509 公开密钥基础设施证书策略和证书业务框架”（Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework），即由互联网标准组织“互联网工程工作组”（Internet

Engineering Task Force) 制定的 RFC3647 标准。RFC3647 框架已经成为 PKI 行业中的一个标准。本 CP 服从 RFC3647 标准, 这样使得使用或考虑使用 CMCTN 证书的用户很容易实现证书策略的映射、比较、评估和互操作。在不改变 RFC3647 总体结构的情况下, 在制定本 CP 时可能会对该结构进行扩充, 以适应 CMCTN 认证业务的特定需求。

本 CP (V0.1) 的生效日期是 **2010 年 09 月 10 日**。

1.2 文档名称与标识

1.2.1 名称

本文档中文名称为《中国移动证书信任体系扩展证书策略》, 英文名称为 CMCTN Extension CP, 简称CMCTN ECP。

1.2.2 版本

本 CP 为 CMCTN 发布的第一个版本, 为 CMCTN ECP 0.1 版本, 即版本号 为 V0.1。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构 (CA)

电子认证服务机构 (Certification Authority, 简称CA) 作为可信第三方, 对个人、实体及设备进行主题信息及其它属性与公钥绑定的确认。CA 是向最终用户或其下 CA 签发证书的实体的术语。它的一个特例是根 CA。一个根 CA 是一类证书体系的最高层。

1.3.2 注册机构（RA）

注册机构（Registration Authority，简称 RA）代表 CA 建立起注册过程，鉴别和标识证书申请者的身份，发起或传递证书吊销请求，并代表 CA 批准更新证书或更新密钥的申请。在订户获得证书前作为中国移动 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。上级 CA 最终决定是签发还是拒绝该订户的申请。如果签发证书，则证书将被发送给申请者。

此外，RA 还须对下层注册分支机构和下层受理点进行管理与提供相应服务，并对于订户的信息与数据 RA 也必须进行妥善保存与做好相关保密工作。

1.3.3 受理点（LRA）

根据业务发展需要以及 CMCTN 地域或行业的划分情况，RA 可以授权建立自身的受理点或注册分支机构（LRA）。

在面向公众提供认证服务前，LRA 必须首先通过 CMCTN 的认证机构的审查，并须与 CMCTN 的认证机构签署 CA 受理点授权协议书。在提供认证服务时 LRA 必须按照 CMCTN 的认证机构当前的证书策略以及授权协议书中的相关约定来办理和审批数字证书申请。

对于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式（通信地址、电子邮件信箱、电话等），LRA 必须向 CMCTN 的认证机构或经 CMCTN 的认证机构授权的注册机构或注册分支机构进行提交，且在开展具体的认证服务时 LRA 也必须根据这些信息来为申请实体制作证书与提供相应的技术支持。

1.3.4 订户

CMCTN 订户即证书所有人，包括所有由 CMCTN 的认证机构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CP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 CMCTN 的认证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 CMCTN 的证书订户，也可以不是订户。

依赖方享有相应的利益，包括 CMCTN 的认证机构可能提供的证书保障，以及 CMCTN 的认证机构的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

以上未提及的隶属于 CMCTN 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

本 CP 阐述的证书类型为中国移动 CMCA 在基线证书标准基础上针对中国移动业务特性提供的扩展型证书，提供基于移动互联网络和移动电子商务的移动安全认证解决方案，为中国移动用户提供安全认证服务。

1.4.1 证书类型和应用范围

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) 手机实名认证证书

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（即应用软件）开发者提供的扩展数字证书。

- 开发者可以为开发者或企业开发者
- 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，企业开发者将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使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。

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** 不对测试证书进行鉴证审核，不承担测试证书的法律风险，本 **CP** 将不对测试证书进行描述。

1.4.2 限制的证书应用

证书禁止在任何违反国家法律、法规或破坏国家安全的情形下使用，否则由

此造成的法律后果由订户自己承担。

CMCTN 的认证机构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，而不能作为设备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，如最终订户证书不能作为 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 CP 限定的应用范围，将是不受保护的。

1.4.3 受禁的证书应用

CMCTN 的认证机构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 CP 由卓望数码技术（深圳）有限公司成立的中国移动 CMCA 认证中心制定，并由该机构下设的安全认证策略管理委员会进行管理。

1.5.2 联系人

本 CP 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，由专门的 CP 管理人员实行日常维护，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：86-755-26718666

传真：86-755-26984689

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 CP 符合策略的机构

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

1.5.4 CP 批准程序

在 CMCTN 证书策略做出任何变动之前，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证书信任体系证书策略文档。

1.6 定义和缩写

CA	电子认证服务机构 (certificate authority)
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)
CMCTN	中国移动证书信任体系 (China Mobile Certificate Trust Network)
CMCA	中国移动 CA (China Mobile Certification Authority)
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)
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的

2.1 信息库

CMCTN 的认证机构或注册机构应有信息库用于各类信息的发布，如证书策略、认证业务声明、协议、证书、证书吊销列表，并在其电子认证业务规则(CPS)、依赖方协议等中指明有关信息发布、获取的位置。

2.2 信息发布

CMCTN 的认证机构应发布的认证信息包括证书策略(CP)、电子认证业务规则(CPS)、订户协议、依赖方协议、证书及证书状态信息，其中 CP、CPS、订户协议及依赖方协议应能够通过 Web 方式查询到，证书能够通过目录方式(LDAP)查询，而 CRL 可通过 LDAP 或 Web 进行查询。

2.3 发布的时间或频率

证书策略、认证业务声明、订户协议、依赖方协议的当前版本，应随时可通过信息库获得。如果进行版本升级，则应在更新版本的生效日期前发布出来，版本升级可不定期进行。在订户进行证书申请注册时，阅读并同意订户协议是成功注册的一个条件。订户证书一经签发即发布到证书信息库，而 **CRL** 的发布周期不应超过 24 小时。

2.4 信息库访问控制

发布在信息库中的信息是对外公开的，任何人都能够查阅，对这些信息的只读访问应该是不受任何限制的，但对于 **CRL** 的访问应以接受依赖方协议作为一个前提条件。

CMCTN 的认证机构应通过物理和逻辑上的安全控制措施防止未经授权的增加、删除或修改信息库的内容。

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，CMCTN 的认证机构签发的证书的主体名字可以是手机号码、人员姓名、企业名称等，命名应符合 X.501 甄别名规定。

甄别名包含于每张证书的主题中，唯一标识证书用户的身份，证书格式应符合 X509.3 标准。

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 CMCTN 的认证机构所有证书持有者都是唯一的。CMCTN 的认证机构接受唯一的甄别名，可根据 DN 鉴别证书持有者。

3.1.2 对名称有意义的要求

对于手机号码证书，如果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，则 CMCTN 的认证机构对甄别名中的关键信息即手机号码进行鉴别。

手机用户个人证书主体甄别名中的通用名可作为标识订户的关键信息被鉴别和认证。

终端应用开发者标识证书主体甄别名的通用名可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

手机号码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

CMCTN 的认证机构应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 手机号码的鉴别

CMCTN 的认证机构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，但是中国移动 CMCA 不确认、不担保签发的证书中除手机号以外的其他身份信息是真实的、可靠的、属于申请者本人的。

3.2.3 手机用户个人身份的鉴别

手机用户申请手机实名证书时，应对提交的证书申请资料的准确性和真实性承担责任。

CMCTN 的认证机构或其授权机构应按照如下方式审核个人身份：

- 1) 申请者需向 CMCTN 的认证机构提供有效身份证明文件
- 2) 核对证书申请资料与有效文件或第三方数据库的资料是否相符
- 3) 如申请者授权经办人申请数字证书，CMCTN 的认证机构或其授权机构还需审核经办人的身份和资格
- 4) 如果 CMCTN 的认证机构或其授权机构已经预先明确了个人的身份，那么 CMCTN 的认证机构或其授权机构可以信赖这些证明
- 5) CMCTN 还须通过手机服务密码、激活验证码等方式验证其手机号码的真实性和有效性

对于个人证书，CMCTN 的认证机构还应确认申请人知晓证书申请。

3.2.4 移动终端设备身份的鉴别

个人或企业用户在申请移动终端设备证书时，需要提供设备相关属性信息，CMCTN 的认证机构或其授权机构通过证明设备产生私钥来验证设备有效性，并根据需要验证设备属性的真实性。如需要验证设备持有人身份，则分别按照个人身份和企业身份进行鉴证，并应确认持有人知晓并授权证书申请。

CMCTN 的认证机构或其授权机构应按照如下方式审核个人身份：

- 1) 申请者需向 CMCTN 的认证机构提供有效身份证明文件。
- 2) 核对证书申请资料与有效文件或第三方数据库的资料是否相符。
- 3) 如申请者授权经办人申请数字证书，CMCTN 的认证机构或其授权机构还需审核经办人的身份和资格。
- 4) 如果 CMCTN 的认证机构或其授权机构已经预先明确了个人的身份，那么 CMCTN 的认证机构或其授权机构可以信赖这些证明。

CMCTN 的认证机构或其授权机构应按照如下方式审核组织机构身份：

- 1) 申请者需向 CMCTN 的认证机构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。
- 2) 核对证书申请资料与有效文件或第三方数据库的资料是否相符。
- 3) CMCTN 的认证机构或其授权机构还需审核企业证书代表人的身份和资格。

3.2.5 终端应用开发者身份的鉴别

个人开发者在申请终端应用开发者标识证书时，应对提交的证书申请资料的准确性和真实性承担责任。

CMCTN 的认证机构或其授权机构应按照如下方式审核个人身份：

- 1) 申请者需向 CMCTN 的认证机构提供有效身份证明文件。
- 2) 核对证书申请资料与有效文件或第三方数据库的资料是否相符。
- 3) 如申请者授权经办人申请数字证书，CMCTN 的认证机构或其授权机构还需审核经办人的身份和资格。
- 4) 如果 CMCTN 的认证机构或其授权机构已经预先明确了个人的身份，那

么 CMCTN 的认证机构或其授权机构可以信赖这些证明。

- 5) 中国移动 CMCA 仅根据客户要求，在正确核实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。

对于终端应用个人开发者标识证书证书，CMCTN 的认证机构还应确认申请人知晓证书申请。

企业开发者在申请终端应用开发者标识证书时，应对提交的证书申请资料的准确性和真实性承担责任。

CMCTN 的认证机构或其授权机构应按照如下方式审核组织机构身份：

- 1) 申请者需向 CMCTN 的认证机构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。
- 2) 核对证书申请资料与有效文件或第三方数据库的资料是否相符。
- 3) CMCTN 的认证机构或其授权机构还需审核企业证书代表人的身份和资格。
- 4) 中国移动 CMCA 仅根据客户要求，在正确核实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。

对于终端应用企业开发者标识证书，CMCTN 的认证机构还应确认该组织机构知晓并授权证书申请。

3.2.6 终端应用身份的鉴别

终端应用即手机终端应用软件，可以通过验证中国移动终端应用认证中心的身份、验证开发者标识证书对终端应用的签名以及中国移动终端应用测试认证中心的测试结果来鉴别终端应用的身份。

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。CMCTN 的认证机构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，CMCTN 的认证机构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。

对于 CMCTN 的认证机构的证书认证业务，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

CMCTN 的认证机构应对常规密钥更新请求进行正确标识和适当鉴别，以保证订户身份的持续有效性。

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，其操作应与证书申请相同。

3.4 吊销请求的标识与鉴别

在 CMCTN 的认证机构的证书业务中，证书吊销请求可以来自订户，也可以来自 CMCTN 的认证机构或其注册机构。证书吊销的方式可以是订户自己吊销，也可以由订户要求 CMCTN 的认证机构或其注册机构管理员吊销，CMCTN 的认证机构和其注册机构在认为必要的时候，有权发起吊销订户证书。

CMCTN 的认证机构应在订户协议中写明对证书吊销请求的鉴别方法。证书吊销的申请者必须满足下列条件之一：

- 1) 提供初始身份验证时的申请材料；或
- 2) 证明拥有需要吊销证书的私钥。

CMCTN 的认证机构或其授权机构应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

4.1 证书申请

4.1.1 证书申请实体

证书申请可由证书拥有实体或相应的授权人提交。

4.1.2 注册过程与责任

证书申请者应向 CMCTN 的认证机构提供真实、完整和准确的信息，以及相应的公钥。申请者还应明确表示同意订户协议中的内容。

4.2 证书审核

4.2.1 执行识别与鉴别功能

当 CMCTN 的认证机构接受到订户的证书申请后，应按§ 3.2 的要求，对订户进行身份识别与鉴别。

4.2.2 证书申请批准和拒绝

CMCTN 的认证机构应根据鉴别的结果批准或拒绝证书申请者的申请。如果拒绝申请，则应该通过适当的方式、在合理的时间内通知证书申请者。

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，CMCTN 的认证机构应在合理的证书请求处理时间内完成证书申请的处理。

4.3 证书签发

4.3.1 签发证书

CMCTN 的认证机构接受订户的证书申请后，应基于审核通过的信息进行证书签发。

4.3.2 拒绝签发证书

CMCTN 的认证机构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，CMCTN 的认证机构在拒绝签发证书后，应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

在数字证书签发完成后，CMCTN 的认证机构可通过安全途径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。

4.4.2 证书的发布

一旦证书申请者接受证书，CMCTN 的认证机构应在信息库或目录服务器里发布证书的副本。证书申请者也可以在其它信息库中公布他们的 CMCTN 的认证机构证书。

4.5 密钥和证书的使用

4.5.1 订户私钥和证书的使用

订户密钥对和证书须用于其规定的、批准的用途。签名密钥对用于签名与签名验证，加密密钥对用户加密解密。如果密钥对允许用于身份鉴别，则可以用于身份鉴别。密钥对和证书不应用于其规定的、批准的用途之外的目的，否则其应用是不受保障的。

证书持有人应按 CP § 6.1, 6.2, 6.4 妥善保管其证书私钥。

4.5.2 依赖方公钥和证书的使用

获得对方的证书和公钥后，依赖方可以通过查看证书以了解对方的身份，通过公钥验证对方电子签名的真实性，实现通信的不可抵赖性，并实现通信双方数据传输的保密性和完整性。

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

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。证书订户必须在证书有效期到期前，向 CMCTN 的认证机构提交申请更新证书。

4.6.1 证书更新的原因

- 证书的使用期限将要到期
- 其他原因

4.6.2 请求证书更新的实体

订户或其授权代表可以请求证书更新。

4.6.3 证书更新流程

CMCTN 的认证机构应提供现场更新或在线更新等不同方式。更新程序根据 CMCTN 的认证机构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。

4.6.4 对更新证书的发布

一旦证书申请者接受了新证书，CMCTN 的认证机构应在信息库或目录服务器里发布证书的副本。证书申请者也可以在其它信息库中公布他们的 CMCTN 证书。

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。

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 CMCTN 的认证机构的义务；
- 2) 原有证书到期，根据订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：

- 证书订户 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。

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订户怀疑自己的密钥失密；
- 3) 与密钥相关的订户的主题信息改变，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) 订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) 订户申请初始注册时，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) 订户申请吊销证书时填写的其他原因。

此外，CMCTN 的认证机构还可能因为法律或政策的要求对订户证书进行强制吊销，此类吊销完成后必须立即通知该证书订户。

4.9.2 请求证书吊销的实体

由 CMCTN 的认证机构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 CMCTN 的各类证书的有效期限未到的证书订户。

CMCTN 的认证机构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 CMCTN

的认证机构或授权的注册机构发起请求,由 CMCTN 的认证机构或授权的注册机构进行吊销。

CMCTN 的认证机构在接到最终订户的吊销请求后,需通过可靠的方式确认请求确实来自最终订户。

CMCTN 的认证机构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 策略对终端订户的证书执行吊销操作。

4.9.4 吊销请求宽限期

CMCTN 的注册机构强制吊销可以给予 24 小时的宽限期。终端订户申请吊销时,CMCTN 的注册机构应在收到吊销请求 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

CMCTN 的认证机构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 CMCTN 的认证机构最新公布的 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 CMCTN 的认证机构发行并数字签名的。

依赖方应根据 CMCTN 的认证机构公布的最新 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

CMCTN 的认证机构应通过证书黑名单库 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。

4.9.8 在线状态查询要求

CMCTN 的认证机构应能提供在线状态查询（OCSP）以实现对证书状态的实时查询。

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；
- 其他，例如：证书订户由于某种原因如长期出差，短期内无法使用证书，可以申请证书挂起。

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 CMCTN 的认证机构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 CMCTN 各类证书的有效期限未到的证书订户。

CMCTN 的认证机构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

证书挂起操作可由证书订户自行进行，也可由证书订户或依赖方向 CMCTN 的认证机构或授权的注册机构发起请求，由 CMCTN 的认证机构或授权的注册机构进行挂起。

CMCTN 的认证机构在接到最终订户的挂起请求后，需通过可靠的方式确认请求确实来自最终订户。

CMCTN 的认证机构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 策略对终端订户的证书执行挂起操作。

4.10.4 挂起的期限限制

CMCTN 的认证机构应在 CPS 中说明证书挂起的最长周期，并提醒证书订户及时恢复证书，如确定不再使用，CMCTN 的认证机构应吊销证书。

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 CMCTN 的认证机构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 CMCTN 的认证机构各类证书的有效期限未到的证书订户。

CMCTN 的认证机构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

证书解挂操作可由证书订户自行进行，也可由证书订户或依赖方向 CMCTN 的认证机构或授权的注册机构发起请求，由 CMCTN 的认证机构或授权的注册机构进行证书解挂。

CMCTN 的认证机构在接到最终订户的解挂请求后，需通过可靠的方式确认请求确实来自最终订户。

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 CMCTN 的认证机构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 CMCTN 的认证机构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

CMCTN 的认证机构应对订户提交的密钥恢复申请进行审核,通过后方可为订户恢复密钥。

4.13 证书状态服务

CMCTN 的认证机构应提供 CRL 发布和 OCSP (在线证书状态查询) 服务两种证书状态服务方式。

CMCTN 的认证机构提供的证书状态查询必须以网络服务的形式,让依赖方能够随时查询、下载。CRL 的发布频率和延迟必须符合 CP § 4.9.7 和 § 4.9.8。

证书状态查询应能立即反映证书的当前状态。证书状态服务的提供应该使标准、通用的方式。对服务请求应该有合理的响应时间和并发处理能力。

4.14 CA 服务终止

CA 服务终止是指证书订户终止与 CMCTN 的认证机构的服务,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) CMCTN 的认证机构将根据证书订户的要求吊销证书。证书订户与 CMCTN 的认证机构的服务终止。

4.15 密钥生成、备份与恢复

证书订户的加密密钥在证书订户申请证书时，由 CMCTN 的认证机构的 KMC 管理中心生成，并进行托管备份，当证书订户需要恢复加密密钥时，由 CMCTN 的认证机构通过 KMC 为订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。

为保证订户签名私钥的安全性，CMCTN 的认证机构不保管签名私钥。因此，要求订户妥善保管、备份签名私钥。由于签名私钥遗失所造成的损失由证书订户自己承担，CMCTN 的认证机构概不负责。

5. 认证机构设施、管理和操作安全控制

5.1 物理安全控制

5.1.1 物理场地安全

CMCTN 的认证机构机房应满足基础标准和建筑物标准，并按照相关法规要求将认证机构进行物理安全区域的划分。所有机房的建设应采用高安全性的监控技术，如视频实时监测、指纹、身份识别卡等监控技术，以确保物理通道的安全。机房内部应只允许经过 CMCTN 的认证机构授权的人员才能进入。

监控系统应能记录安全区域的所有进出情况。

5.1.2 物理访问

CMCTN 的认证机构的门禁系统能够通过身份识别卡和指纹鉴别实现访问控制，防止物理非法进入。

5.1.3 电力与空调

CMCTN 的认证机构的安全设施需要主、备电力供应系统，以确保持续不间断的电力供应。同时对于关键的安全设施，也需要主、备空调系统来控制温度和湿度。

5.1.4 水患防治

CMCTN 的认证机构在机房建设应采取相应措施，防止水侵蚀，充分保障系统安全。

5.1.5 火灾防护

CMCTN 的认证机构必须提供火灾自动报警系统和应急处理装置，并符合 GB 50116-98:《火灾自动报警系统设计规范》的要求。

CMCTN 的认证机构应该采取措施并进行相应的设备配置，制定相应的流程，以防止明火或者烟雾对系统造成损害或不利影响。

5.1.6 介质存储

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

当认证机构保存的相关数据已不再需要或存档的期限已满时，CMCTN 的认证机构应及时销毁这些数据。所有处理行为应记录在案，以供审查的需要，销毁

行为应符合法律要求。

5.1.8 异地备份

CMCTN 的认证机构应提供进行安全异地备份的设施，并制定异地备份流程。

5.2 流程安全控制

5.2.1 可信角色

CMCTN 的认证机构应设置执行 CA 系统的关键职能职位，包括但不限于：

- 安全管理员

作为认证机构系统的安全管理员，就是要开发内部过程和具体操作，以满足本本文中提出的指导方针。

CMCTN 的认证机构的 CA 安全管理员负责日常的安全工作：

- 1) 制定认证机构的安全策略；
- 2) 指导认证机构的安全管理；
- 3) 设计和指导认证机构的安全策略实施；
- 4) 对认证机构的安全管理进行定期的检查和评估；
- 5) 对安全策略和执行程序的日常维护。

CA 安全管理员对安全的三个关键领域负有全面的责任：

- 1) 开发与执行安全策略；
- 2) 维护与完善安全策略；
- 3) 保持安全审计的一致性。

安全管理人员有责任来定义和委托认证机构的特定个人和部门的安全职责。

- 审计管理员

审计管理员拥有对系统事件/日志进行查询、追踪、报告、汇总、删除的权限。审计管理员操作审核子系统对整个系统状态进行掌握。审计管理员可以删除过期日志，但无法删除“删除日志”这一事件，这样做是为了保证所有事件的可跟

踪性。审计管理员拥有以下权限：

- 1) 读取管理员的访问控制信息；
- 2) 查询系统日志；
- 3) 备份日志。

- 超级管理员

负责认证机构系统的策略设置，设置各子系统的业务管理员并对其管理的业务范围进行授权。超级管理员由系统初始化时产生，主要职责是设置业务管理员并进行管理。其权限为：

- 增加业务管理员；
- 注销业务管理员；
- 设置业务管理员权限；
- 修改业务管理员权限。

CA 超级管理员拥有对其他管理员管理的权限以及 CA 证书的更新权限，但没有任何其他操作权限。所有其他操作员的设置和权限分配都是由超级管理员来执行的。

- 业务管理员

业务管理员拥有对其系统内部各操作员管理的权限，包括对操作员的设置和权限分配都由业务管理员来执行。系统分别设置 CA 业务管理员和 RA 业务管理员，CA 业务管理员负责对 CA 业务操作员的设置和权限分配，RA 业务管理员负责对 RA 业务操作员和 LRA 业务操作员的设置和权限分配。

- 业务操作员

业务操作员按其权限进行相应的业务操作，分为 CA 操作员、RA 操作员、LRA 操作员。

CA 操作员负责对整个认证机构以及下级 RA 的业务数据进行查询、统计、分析等操作。

RA 操作员负责对本注册机构的业务数据的一些管理操作。

LRA 操作员主要面向订户和证书受理机构，处理来自订户的各种申请，因此享有较多的权限。

安排上述职位是为了确保责任明确，建立有效的安全机制，保证内部管理和

操作的安全。

CMCTN 的认证机构根据受理点的章程，规范受理点操作人员的操作。在受理点的软件设计中，充分考虑安全的牵制和约束。CMCTN 的认证机构对受理点的责任进行合理划分，并在系统、技术实现以及管理的责任义务上保证。

5.2.2 每项任务需要的人数

CMCTN 的认证机构应确保单个人不能接触、导出、恢复、更新、吊销 CMCTN 的 CA 系统存储的根证书对应的私钥，并且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。

CMCTN 的认证机构应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 CMCTN 的认证机构应对在职人员执行重要操作之前进行身份的识别与鉴别，可通过各种安全令牌标示。CMCTN 的认证机构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

CMCTN 的认证机构应对重要岗位的操作进行职责分割，防止误操作或是协同作弊行为的发生。

5.3 人员控制

5.3.1 资格、经历和无过失要求

CMCTN 的认证机构应要求可信人员，提供有关教育背景、工作资格以及相关从业经历的证明。如果需要，也应要求可信人员提供无犯罪证明。

CMCTN 的认证机构应对人员的教育水平、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

CMCTN 的认证机构应制定员工背景审查程序，对员工的录取进行严格的审查，根据岗位需要对员工进行可信背景审查，并定期进行复审。

5.3.3 培训要求

CMCTN 的认证机构应对其人员进行培训，培训内容与人员对应职责相关，包括：使用、操作和维护电子认证服务系统过程中涉及的职责、安全机制（例如：灾难恢复的方法、业务连续性要求）以及电子认证服务系统的软硬件操作规范，以及相关法律法规。

5.3.4 再培训周期和要求

CMCTN 的认证机构应根据行业法律法规、认证机构策略调整、系统更新等情况，对员工进行继续培训，以适应新的变化。

5.3.5 岗位分离和轮换

CMCTN 的认证机构可根据岗位的职责内容和安全要求制定分离和轮换方式。

5.3.6 未授权行为的处罚

CMCTN 的认证机构应在得到员工违规消息后立即中止该员工进入认证机构。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，认证机构立即终止该人员的工作。

5.3.7 提供给员工的文档

CMCTN 的认证机构应为所有员工提供的文档包括：岗位职责、业务操作说明和电子认证服务机构安全管理的相关规范等。

5.4 安全审计

5.4.1 记录事件的类型

CMCTN 的认证机构应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。

- CMCTN 的认证机构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

日志记录应包括如下信息：

- 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

CMCTN 的认证机构应对记录进行定期审查，对审查记录行为备案。

5.4.3 审计日志的保存期限

CMCTN 的认证机构在数据库保存审查记录应不少于三个月，离线存档不少于五年。

5.4.4 审计日志的保护

CMCTN 的认证机构应制定严格的访问控制管理流程，确保只有 CMCTN 的认证机构授权的人员才能接近这些审查记录。

5.4.5 审计日志备份程序

CMCTN 的认证机构应制定合适的备份策略，定期对日志进行备份。

5.4.6 审计收集系统

CMCTN 的认证机构应保证审计日志收集系统 7X24 小时可访问，以在需要的时候，可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

CMCTN 的认证机构应对审查中发现的攻击现象做详细记录，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。

5.4.8 脆弱性评估

应对在审查过程中发现的系统的脆弱性进行评估，出具评估报告，并及时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，应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

CMCTN 的认证机构应对 CA 的数据库定期归档，归档间隔时间可由 CMCTN 的认证机构自行决定，存档的内容包括 CMCTN 的认证机构发行的证书

和 CRL、审查数据记录、证书申请审批资料等。

5.5.2 归档记录的保存期限

CMCTN 的认证机构的归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

应对归档内容实施适当的保护措施，确保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。

应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。

应每年会验证归档信息的完整性。

5.5.4 归档文件的备份

应对归档文件的数据库进行异地备份，并确保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。

CMCTN 的认证机构应设置安全机制防止对档案及其备份进行非授权的删除、修改等操作。

5.5.5 记录时间戳要求

所有存档内容都应加时间标识。

5.5.6 归档收集系统

CMCTN 的认证机构的档案收集系统可由人工操作和自动操作两部分组成。

5.6 密钥更替

CA 密钥（根密钥）的更替，必须上报电子认证服务管理部门，并在其监督下进行重新生成新的密钥，并将自签名证书上交电子认证服务管理部门备案。

新的 CMCTN 的认证机构应继续使用旧的 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

CMCTN 的认证机构应针对事故的性质制定和实施灾难恢复流程，可考虑建立异地灾备中心，以在关键设备和数据遭受破坏时能够及时进行恢复，保持业务持续性。

当发生私钥泄露事件时，CMCTN 的认证机构应立即对其进行吊销。

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

CMCTN 的认证机构可根据密钥受损原因和非密钥受损原因终止业务。

5.8.2 终止通知

当 CMCTN 的认证机构打算终止经营时，应在终止经营前三个月给 CMCTN 的认证机构授权的注册机构、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

CMCTN 的认证机构应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 RA 的终止

根据 CMCTN 的认证机构与注册机构签订的协议终止 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

6.1.1 CA 密钥对的产生

CMCTN 的认证机构应按照密钥管理操作流程和安全要求，由专门人员在 CMCTN 的认证机构核心区屏蔽机房内的离线操作区产生 CA 密钥对。CMCTN 的认证机构的密钥对应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

加密密钥对应由中华人民共和国国家密码管理局许可的、CMCTN 的认证机构数字证书签发系统支持的加密机设备生成的，由 CMCTN 的认证机构所属的 KMC 控制管理。

签名密钥对应由订户端产生，证书申请者应使用国家密码管理局认可的、CMCTN 的认证机构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 CMCTN 的认证机构无法复制签名密钥对。

6.1.3 私钥传送

如果订户自己生成密钥对，则不需要私钥传递。

如果是 CMCTN 的认证机构代表订户生成私钥，必须安全地递交给订户。如果密钥对在 CMCTN 的认证机构提供的硬件令牌中生成，分发这些令牌必须采取合理的方式提供物理安全防护措施，防止令牌中的私钥丢失、泄露、修改或者进行未授权的访问，也必须采取合理的方式确保私钥在未被订户接受前不能被激活。

6.1.4 公钥传送

对于加密证书,CMCTN 的认证机构从 KMC 取得订户公钥后为其签发证书,在此过程中应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,订户应通过 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 CMCTN 的认证机构(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

CMCTN 的认证机构的根公钥包含在 CMCTN 的认证机构根证书中,应向证书订户提供安全的下载方式,以便订户获取 CMCTN 的认证机构根证书。

6.1.6 密钥的长度

CMCTN 的认证机构所使用的密钥对长度应至少为 2048 位。

中国移动订户所使用的密钥长度应至少为 1024 位。

6.1.7 公钥参数的生成

公钥参数应由国家密码管理局许可的、CMCTN 的认证机构数字证书签发系统支持的硬件产生。

6.1.8 密钥用途

CMCTN 证书服务体系中的密钥用途应和证书类型紧密相关,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	终端应用企业开发 者标识证书	终端应用个人开发 者标识证书	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	CodeSigning	\	\	\	\	\	\	\

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

CMCTN 的认证机构应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

CMCTN 的认证机构应采用 M 选 N 多人控制策略激活、使用、停止 CMCTN 的认证机构的签名密钥。

6.2.3 私钥托管

CMCTN 的认证机构应根据订户和法律的需要，对订户加密密钥提供托管服务。签名私钥不应进行托管，以保证其不可否认性。

6.2.4 私钥备份

证书订户应备份他们的私钥，以确保这些私钥的安全。KMC 应备份托管的

加密私钥，确保加密私钥的安全。

6.2.5 私钥归档

KMC 应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

CMCTN 的认证机构应允许把加密私钥导入密码模块中，但应禁止私钥从密码模块中导出；应采取适当措施，使得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，例如将私钥保存在硬件密码模块中。CMCTN 的认证机构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 最终订户证书私钥

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

6.2.8.2 运营设备证书私钥

对于 CMCTN 的认证机构的运营设备证书私钥的激活同 CA 私钥的激活；对于 CMCTN 的认证机构注册机构的运营设备证书私钥，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

CMCTN 的认证机构的 CA 私钥必须存放在硬件密码模块中，并且其激活数

据按 CP § 6.2.2 进行分割。当需要使用 CA 私钥时（在线或离线），需要 CMCTN 的认证机构 CA 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。

6.2.9 解除私钥激活状态

对于手机号码证书、手机实名证书以及终端应用开发者标识证书，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）、或订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。

对于移动终端设备证书等设备证书，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。

6.2.10 销毁私钥

在 CA 私钥生命周期结束后，CMCTN 的认证机构应将 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 私钥的销毁应确保 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

CMCTN 的认证机构应对所有的公钥进行归档处理，并保证公钥的安全性。

6.3.2 证书操作期和密钥对使用期

CMCTN 的认证机构应在订户申请审核鉴定通过后及时将证书颁发给订户，密钥对的使用期限与证书有效期相一致，一般为 1 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 CMCTN 的认证机构提供的口令、被加密的数据等。CMCTN 的认证机构应提供唯一的不可猜测的口令。这些口令由 CMCTN 的认证机构根据授权和操作的许可仅发放给授权订户。

6.4.2 敏感数据的保护

CMCTN 的认证机构应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。未授权订户企图使用敏感数据达到预定目的时，敏感数据应自动锁定。

6.5 计算机安全控制

6.5.1 计算机安全技术要求

CMCTN 的认证机构的数字证书签发系统的数据文件和设备应由 CMCTN 的认证机构系统管理员维护，未经 CMCTN 的认证机构管理员授权，其它人员不能操作和控制 CMCTN 的认证机构系统；其它普通订户无系统账号和密码。CMCTN 的认证机构系统应部署在多级不同厂家的防火墙之内，确保系统网络安全。CMCTN 的认证机构系统密码应有最小密码长度要求，而且必须符合复杂度要求，CMCTN 的认证机构系统管理员定期更改系统密码。

CMCTN 的认证机构系统内的计算机均应采用如防火墙、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，充分保证计算机的安全可靠。

6.5.2 计算机安全评估

CMCTN 的认证机构使用的密码设备应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、系统软件等应通过国家相关部门的检测，属合格产品。

6.6 网络的安全控制

CMCTN 的认证机构应有防火墙以及其他访问控制机制保护，其配置应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 CMCTN 的认证机构员工才能够进入 CMCTN 的认证机构签发系统、CMCTN 的认证机构注册系统、CMCTN 的认证机构目录服务器、CMCTN 的认证机构证书发布系统等设备或系统。所有授权订户必须有合法的安全令牌，并且通过密码验证。

6.7 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

CMCTN 的认证机构签发的证书应符合 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 CP § 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
有效期至	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 CP § 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 CP § 7.1.3 中指定的算法，密钥长度满足 CP § 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

应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 CP§ 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 CMCTN 的认证机构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)

CMCTN 的认证机构证书的基本限制扩展项中的主体类型被设为 `CA`。最终订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。对于最终订户证书签发 `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订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)

对不同的证书，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	终端应用企业开发 者标识证书	终端应用个人开发 者标识证书	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）

CMCTN 的认证机构签发的证书中包含 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

CMCTN 的认证机构最终订户证书及中级 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

CMCTN 的认证机构签发的证书按照 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

CMCTN 的认证机构定期签发 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，CMCTN 的认证机构每隔 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。
有效期	CRL 的签发日期。

域	值或值的限制
下次更新	CRL 下次签发的日期。对于 CA，隔 2 年；对于最终订户证书 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

CMCTN 的认证机构为证书订户提供 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 of 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 认证机构的审计

CMCTN 的认证机构应对自身运营体系包括其关联单位的业务流程和运营操作进行内部审计和监督审计，以检验其是否符合本 CP 和相关规范的规定。

CMCTN 的认证机构还应接受行业主管部门的不定期业务检查与审计。

8.1.2 认证机构对关联单位的审计

CMCTN 的认证机构应对其关联单位实行定期或不定期审计。

CMCTN 的认证机构可保留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的权利。

CMCTN 的认证机构可保留对关联单位的审计收取审计费用的权利。

8.2 审计者的资质

对 CMCTN 的认证机构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 审计者与认证机构的关系

8.3.1 审计者与认证机构的关系

实施规范审计的外部审计者应与 CMCTN 的认证机构是相互独立的,没有任何利益关系。

对 CMCTN 的认证机构及其关联单位实施内部规范审计和监督审计的审计者应为此认证机构独立的审计部门或审计小组。

8.3.2 审计报告与认证机构 的关系

对于内部审计, CMCTN 的认证机构的审计部门或审计小组应提供内部审计报告。

对于外部审计,审计报告的作者是外部审计机构, CMCTN 的认证机构对其内容可不负任何责任,同时 CMCTN 的认证机构也可不对这些审计报告发表任何观点,也可不对由于信任审计报告中有关 CMCTN 的认证机构的内容而导致的任何损失负责。

8.4 审计内容

对 CMCTN 的认证机构的规范审计应包括:

- 1) CMCTN 的认证机构支持的证书认证操作规程是否完全与本证书策略的要求一致。
- 2) CMCTN 的认证机构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 CMCTN 的认证机构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

审计完成后, CMCTN 的认证机构应根据审计的结果检查缺失和不足,根据提出的整改要求,提交修改和预防措施以及整改计划书,并尽快落实执行。

8.6 评估结果的传达与发布

除非法律明确要求，CMCTN 的认证机构可不公开相关审计结果。

对于关联单位的监督审计结果，CMCTN 的认证机构的审计部门应按照本机构的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

CMCTN 的认证机构应根据制定的收费策略向证书订户收取相关费用。如在此收费基础上提出了相关资费优惠政策，CMCTN 的认证机构应向证书申请者或订户进行说明与明确。

9.1.2 退款策略

CMCTN 的认证机构应严格遵守并承担本证书策略所规定的责任，如有违背，则订户可以要求 CMCTN 的认证机构吊销证书并退款。在 CMCTN 的认证机构吊销了订户的证书后，CMCTN 的认证机构应立即将订户为申请该证书所支付的全额费用退还给订户。退款时，订户需要填写退款申请表，并发送给 CMCTN 的认证机构，以要求退款。此退款程序不应限制订户得到其它的赔偿。

9.2 财务责任

CMCTN 的认证机构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。

9.2.1 保险范围

CMCTN 的认证机构应制订自身的投保策略并承担相关责任，投保范围应包括但不限于：

- 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 CMCTN 的认证机构证书订户和证书依赖方保险时间为在证书的有效期内。

9.2.2 对最终实体的保险或担保

CMCTN 的认证机构应对证书最终实体承担保险或担保责任。

9.3 业务信息保密

9.3.1 保密信息范围

保密信息包括以下内容：

- 1) CMCTN 的认证机构与订户之间的协议、往来函件等，未经订户书面许可，不得对任何第三方公开。
- 2) 证书申请材料。
- 3) 审计记录。
- 4) CMCTN 的认证机构系统操作相关的访问控制。
- 5) CMCTN 的认证机构根据合理的商业判断应理解为保密数据和信息的。
- 6) 除非法律明文规定，CMCTN 的认证机构不必公布或透露订户证书以外的信息。

9.3.2 不属于保密的信息

不属于保密的信息包括（但不限于）以下内容：

- 1) 电子认证业务规则。
- 2) 与证书有关的申请流程、申请手续、申请操作指南等信息。

- 3) CMCTN 的认证机构目录服务器中公布证书的作废信息。
- 4) 证书、证书内包括的公钥、证书中包括的订户信息。

9.3.3 对业务信息保密的责任

CMCTN 的认证机构、订户、依赖方、关联机构以及其他参与者，都有责任按照本 CP 的规定保证相关保密信息的不被泄漏。

9.4 个人隐私保密

9.4.1 隐私保密方案

对于用户的敏感隐私数据，如手机号码，CMCTN 的认证机构应制定隐私保护方案，以保证不会滥用、未授权使用或出售证书申请者姓名等任何证书申请者资料，并需采取必要的安全措施以防止证书申请者资料被遗失、盗用与篡改。

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，特别是用户手机号码，非经订户同意或者法律法规及公权力部门的合法要求，CMCTN 的认证机构不得任意对外公开。

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

CMCTN 的认证机构、订户、依赖方、关联机构以及其他参与者，都有责任按照本 CP 的规保护隐私信息不被泄漏。

9.4.5 依法律或行政程序的信息披露

由于法律执行、法律授权的行政执行的需要，CMCTN 的认证机构可进行信息披露。

9.4.6 其他信息披露情形

在信息所有者书面授权的情况下 CMCTN 的认证机构可向特定对象进行信息披露。

9.5 知识产权

CMCTN 的认证机构享有并保留除 CMCTN 的认证机构系统软件之外的知识产权，包括 CMCTN 的认证机构的名称权、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 CMCTN 的认证机构的同意后，可以使用相关的文件 and 手册，并有责任和义务提出修改意见。

在没有 CMCTN 的认证机构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 CMCTN 的认证机构使用的名称、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 认证机构的责任和义务

CMCTN 的认证机构应承担的唯一和绝对的责任和义务是：

- 保证 CMCTN 的认证机构 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 CMCTN 的认证机构 的签名私钥在 CMCTN 的认证机构 CSF 内部

得到安全的存放和保护；

- CMCTN 的认证机构 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，CMCTN 的认证机构、CMCTN 的认证机构的服务机构、CMCTN 的认证机构授权的注册机构、CMCTN 的认证机构 的雇员不承担其它任何义务。必须指出，本证书策略的内容，没有任何信息可以暗示或解释成 CMCTN 的认证机构 必须承担其它的义务或 CMCTN 的认证机构 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

CMCTN 的认证机构 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，CMCTN 的认证机构 由于受到影响，可免除第 9.6.1.1 条款、本证书策略以及其它相应证书策略所规定的责任和义务。

9.6.2 注册机构的陈述与担保

注册机构必须遵守所有的登记程序和安全保障措施。这些程序和保障由 CMCTN 的认证机构 决定，并在本证书策略或相应的注册机构协议中规定，以后 CMCTN 的认证机构 可以根据情况修改有关内容，并及时公布。

注册机构必须遵守和符合本证书策略的条款。

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：

- 在申请证书时，订户提交的所有陈述和信息都是真实的；
- 证书订户同意严格遵守和服从认证业务声明规定的或者由 CMCTN 的认证机构推荐使用的安全措施；
- 证书订户需熟悉与证书相关的证书政策和认证业务声明的条例，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，证书订户应立刻通知 CMCTN 的认证机构或认证机构授权的注册机构，并申请采取相关处理措施。

9.6.4 依赖方的陈述与担保

依赖方在信赖 CMCTN 的认证机构证书的时候，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均需要遵守本证书策略。

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 CMCTN 的认证机构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，CMCTN 的认证机构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。

CMCTN 的认证机构不必承担任何其他未经授权的人或组织以 CMCTN 的认证机构名义编撰、发表或散布不可信赖的信息所引起的法律责任。

CMCTN 的认证机构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。

CMCTN 的认证机构不必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 CMCTN 的认证机构自身原因，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，CMCTN 的认证机构将承担相应的赔偿责任，但这种责任是有限的。

CMCTN 的认证机构在对外服务过程中只承担对外声明的、本 CP 中规定的、对外签署的任何协议中所规定的有限责任。CMCTN 的认证机构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 CMCTN 的认证机构违反了规定的职责，CMCTN 的认证机构应承担赔偿责任（法律免责除外）。

9.9.1 赔偿条件

有下列情形之一的，CMCTN 的认证机构应承担有限的赔偿责任：

- 1) 由于 CMCTN 的认证机构的未授权使用或泄露造成的客户私钥泄露，CMCTN 的认证机构进行赔偿；
- 2) 当 CMCTN 的认证机构由于故意违反本 CP 造成的客户的经济损失，CMCTN 的认证机构进行赔偿；
- 3) 由于 CMCTN 的认证机构自身原因造成的颁发给客户的证书信息出现

实质性错误，CMCTN 的认证机构进行赔偿。CMCTN 的认证机构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 CMCTN 的认证机构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的，给CMCTN的认证机构、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，依赖方应对自身原因造成的CMCTN的认证机构损失承担责任：

- 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，CMCTN的认证机构不承担赔付责任：

- 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，CMCTN的认证机构所应承担的有限责任的赔偿限额如下：

证书类型	赔偿限额
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) CMCTN 的认证机构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 CMCTN 的认证机构改动。
- 2) CMCTN 的认证机构只有在 CA 证书有效期限内承担这种损失或损害赔偿。
- 3) CMCTN 的认证机构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

注册机构的责任应在注册机构和 CMCTN 的认证机构之间签定的注册机构协议中进行明确。

9.10 有效期限与终止

CMCTN 的认证机构 的 CP 自发布之日起正式生效，当新版本的 CP 正式发布生效，则旧版本的 CP 将自动终止。

9.11 修订

CMCTN 的认证机构保留对本证书策略中的任何术语、条件和条款进行随时修订的权利，且可无须预先通知任何一方，但对于修订后的证书策略，CMCTN

的认证机构必须及时进行公布。

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

本证书策略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，本证书策略的执行、解释、翻译和有效性均适用中华人民共和国的法律。

9.15 一般条款

9.15.1 完整协议

不作规定。

9.15.2 转让

不作规定。

9.15.3 分割性

本 CP 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 CP 其余的部分（以及对它方的无效或不能执行的条款的适

用) 将能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, 本 CP 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

CMCTN 的认证机构和发证机构可不对以下超越它们控制能力的事件所造成 CMCTN 的认证机构的 CP 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

CMCTN 的认证机构与具体客户协商后可另行确定其他条款, 包括未在上述说明的其他相关内容条款。