重庆程远未来电子商务服务有限公司
电子认证业务规则

重庆程远未来电子商务服务有限公司

2018 年 10 月

程远未来
iFuture Service

□内部保密

■ 公开

程远未来
电子认证业务规则

编号：CYWL-II01-2018

版本号：V1.2

重庆程远未来电子商务服务有限公司

发布日期： 2018 年 10 月 19 日

公开

【文档信息】

文档名称	程远未来电子认证业务规则		
文档编号	CYWL-II01-2018		
关联文档(上级)	程远未来通用分类证书策略(CP)		
关联文档(下级)			
保密级别	公开	**文档版本号**	V1.2
制作人	CPS 编写小组	**制作日期**	2018.10.12
复审人	安全策略委员会	**复审日期**	2018.10.18
批准人	安全策略委员会	**批准日期**	2018.10.18
发布人	安全策略委员会	**发布日期**	2018.10.19
受控状态	■是　　□否		

【版本变更记录】

生效日期	**版本**	**修改说明**	**修改人**	**复审人**	**批准人**
2017 年 3 月	V1.0	创建	黄雪梅	安全策略委员会	安全策略委员会
2018 年 6 月	V1.1	1、修订了名词和术语； 2、依据《证书策略》全面修订内容； 3、调整文档格式。	徐蕤、刘磊、刘玉祥、李海波、魏薇	安全策略委员会	安全策略委员会
2018 年 10 月	V1.2	1、完善线上鉴别验证方式及其对应的业务流程； 2、修订免责条款等。	徐蕤、刘磊、刘玉祥、李海波、魏薇	安全策略委员会	安全策略委员会

目　　录

1　概括性描述.....1
1.1　概述.....1
1.2　文档名称与标识.....1
1.3　电子认证活动参与方及其职责.....1
1.3.1　电子认证服务机构.....1
1.3.2　注册机构.....1
1.3.3　订户.....2
1.3.4　依赖方.....2
1.3.5　其他参与者.....3
1.4　证书应用.....3
1.4.1　适合的证书应用.....3
1.4.2　受限的证书应用.....3
1.4.3　禁止的证书应用.....4
1.5　策略管理.....4
1.5.1　策略文档管理机构.....4
1.5.2　联系人.....4
1.5.3　决定 CPS 符合策略的机构.....4
1.5.4　CPS 批准程序.....5
1.5.5　CPS 修订.....5
1.6　定义和缩写.....5
2　信息发布与信息管理.....8
2.1　认证信息的发布.....8
2.2　发布时间或频率.....8
2.3　信息库访问控制.....8
3　身份标识与鉴别.....9
3.1　命名.....9
3.1.1　名称类型.....9
3.1.2　对名称意义化的要求.....9
3.1.3　订户的匿名或伪名.....9
3.1.4　理解不同名称形式的规则.....10
3.1.5　名称的唯一性.....10
3.1.6　商标的承认、鉴别和角色.....10
3.2　初始身份确认.....10
3.2.1　证明持有私钥的方法.....10

3.2.2 机构身份的鉴别.....10
3.2.3 个人身份的鉴别.....12
3.2.4 没有验证的订户信息.....12
3.2.5 授权确认.....13
3.2.6 互操作准则.....13
3.3 密钥更新请求的身份标识与鉴别.....13
3.3.1 常规密钥更新的标识与鉴别.....13
3.3.2 撤销后密钥更新的标识与鉴别.....14
3.4 撤销请求的标识与鉴别.....14
4 证书生命周期操作要求.....14
4.1 证书申请.....14
4.1.1 证书申请实体.....14
4.1.2 申请过程与责任.....15
4.2 证书申请处理.....15
4.2.1 执行识别与鉴别功能.....15
4.2.2 证书申请批准和拒绝.....16
4.2.3 处理证书申请的时限.....16
4.3 证书签发.....16
4.3.1 证书签发过程中电子认证服务机构的行为.....16
4.3.2 电子认证服务机构对订户的通告.....17
4.4 证书接受.....17
4.4.1 构成接受证书的行为.....17
4.4.2 电子认证服务机构对证书的发布.....17
4.4.3 电子认证服务机构在颁发证书时对其他实体的通告.....18
4.5 密钥对和证书的使用.....18
4.5.1 订户私钥和证书的使用.....18
4.5.2 依赖方对公钥和证书的使用.....18
4.6 证书更新.....19
4.6.1 证书更新的情形.....19
4.6.2 请求证书更新的实体.....19
4.6.3 证书更新请求的处理.....20
4.6.4 颁发新证书时对订户的通告.....20
4.6.5 构成接受更新证书的行为.....20
4.6.6 电子认证服务机构对更新证书的发布.....20
4.6.7 电子认证服务机构在颁发证书时对其他实体的通告.....20
4.7 证书密钥更新.....20

4.7.1 证书密钥更新的情形.....21
4.7.2 请求证书密钥更新的实体.....21
4.7.3 证书密钥更新请求的处理.....21
4.7.4 颁发新证书对订户的通告.....21
4.7.5 构成接受密钥更新证书的行为.....21
4.7.6 电子认证服务机构对密钥更新证书的发布.....21
4.7.7 电子认证服务机构在颁发证书时对其他实体的通告.....21
4.8 证书变更.....22
4.8.1 证书变更的情形.....22
4.8.2 请求证书变更的实体.....22
4.8.3 证书变更请求的处理.....22
4.8.4 颁发新证书时对订户的通告.....22
4.8.5 构成接受变更证书的行为.....22
4.8.6 电子认证服务机构对变更证书的发布.....22
4.8.7 电子认证服务机构对其他实体的通告.....22
4.9 证书撤销和挂起.....23
4.9.1 证书撤销的情形.....23
4.9.2 请求证书撤销的实体.....23
4.9.3 撤销请求的流程.....23
4.9.4 撤销请求宽限期.....24
4.9.5 电子认证服务机构处理撤销请求的时限.....24
4.9.6 依赖方检查证书撤销的要求.....24
4.9.7 CRL 的签发频率.....24
4.9.8 CRL 发布的最长滞后时间.....25
4.9.9 证书状态查询的可用性.....25
4.9.10 撤销信息的其他发布形式.....25
4.9.11 对密钥遭受安全威胁的特别处理要求.....25
4.9.12 证书挂起.....25
4.10 证书状态服务.....25
4.10.1 操作特点.....26
4.10.2 服务可用性.....26
4.10.3 可选特征.....26
4.11 订购结束.....26
4.12 密钥托管与恢复.....26
4.12.1 密钥托管与恢复的策略与行为.....26
4.12.2 会话密钥的封装与恢复的策略与行为.....27

5 电子认证服务机构设施、管理和操作控制.....27
5.1 物理控制.....27
5.1.1 场地位置与建筑.....27
5.1.2 物理访问.....28
5.1.3 电力与空调.....29
5.1.4 水患防治.....30
5.1.5 火灾预防和保护.....30
5.1.6 介质存储.....31
5.1.7 废弃物处理.....31
5.1.8 异地备份.....32
5.2 程序控制.....32
5.2.1 可信角色.....32
5.2.2 每个角色的识别与鉴别.....33
5.2.3 需要职责分割的角色.....33
5.3 人员控制.....34
5.3.1 资格、经历和无过失要求.....34
5.3.2 背景审查程序.....34
5.3.3 培训要求.....34
5.3.4 再培训周期和要求.....35
5.3.5 工作轮换周期和顺序.....35
5.3.6 对未授权行为的处罚.....35
5.3.7 独立合约人的要求.....35
5.3.8 提供给员工的文档.....35
5.4 审计日志处理流程.....36
5.4.1 记录事件的类型.....36
5.4.2 处理或归档日志的周期.....36
5.4.3 审计日志的保存期限.....36
5.4.4 审计日志的保护.....36
5.4.5 审计日志备份程序.....37
5.4.6 审计日志收集系统.....37
5.4.7 对导致事件实体的通告.....37
5.4.8 脆弱性评估.....37
5.5 记录归档.....37
5.5.1 归档记录的类型.....37
5.5.2 归档记录的保存期限.....38
5.5.3 归档文件的保护.....38

5.5.4 归档文件的备份程序.....38
5.5.5 归档记录的时间标记要求.....38
5.5.6 获得和检验归档信息的程序.....38
5.5.7 访问和检验归档记录的流程.....39
5.6 电子认证服务机构密钥更替.....39
5.7 损害和灾难恢复.....39
5.7.1 事故和损害处理程序.....39
5.7.2 计算资源、软件和/或数据的损坏.....40
5.7.3 实体私钥损害处理程序.....40
5.7.4 灾难后的业务连续性能力.....40
5.8 电子认证服务机构或注册机构的终止.....40
6 认证系统技术安全控制.....41
6.1 密钥对的生成和安装.....41
6.1.1 密钥对的生成.....41
6.1.2 私钥传送给订户.....41
6.1.3 公钥传送给证书签发机构.....42
6.1.4 电子认证服务机构公钥传送给依赖方.....42
6.1.5 密钥的长度.....42
6.1.6 公钥参数的生成和质量检查.....42
6.1.7 密钥使用目的.....42
6.2 私钥保护和密码模块工程控制.....43
6.2.1 密码模块标准和控制.....43
6.2.2 私钥多人控制.....43
6.2.3 私钥托管.....44
6.2.4 私钥备份.....44
6.2.5 私钥归档.....44
6.2.6 私钥导入或导出密码模块.....44
6.2.7 私钥在密码模块中的存储.....45
6.2.8 激活私钥的方法.....45
6.2.9 解除私钥激活状态的方法.....45
6.2.10 销毁密钥的方法.....45
6.2.11 密码模块的评估.....45
6.3 密钥对管理的其他方面.....46
6.3.1 公钥归档.....46
6.3.2 证书操作期和密钥对使用期限.....46
6.4 激活数据.....47

6.4.1 激活数据的产生和安装.....47
6.4.2 激活数据的保护.....47
6.4.3 激活数据的其他方面.....47
6.5 计算机安全控制.....48
6.5.1 特别的计算机安全技术要求.....48
6.5.2 计算机安全评估.....48
6.6 生命周期技术控制.....48
6.6.1 系统开发控制.....48
6.6.2 安全管理控制.....49
6.6.3 生命周期的安全控制.....49
6.7 网络的安全控制.....49
6.8 时间标记.....49
7 证书、证书撤销列表和在线证书状态协议.....50
7.1 证书.....50
7.1.1 版本号.....50
7.1.2 算法对象标识符.....50
7.1.3 名称形式.....50
7.1.4 证书扩展项.....51
7.2 证书撤销列表.....51
7.2.1 版本号.....52
7.2.2 CRL 和 CRL 条目扩展项.....52
7.3 在线证书状态协议.....52
7.3.1 版本号.....52
7.3.2 OCSP 扩展项.....52
8 电子认证服务机构审计和其他评估.....52
8.1 评估的频率或情形.....52
8.2 评估者的资质.....52
8.3 评估者与被评估者之间的关系.....53
8.4 评估内容.....53
8.5 对问题与不足采取的措施.....53
8.6 评估结果的传达与发布.....53
9 法律责任和其他业务条款.....54
9.1 费用.....54
9.1.1 证书签发和更新费用.....54
9.1.2 证书查询费用.....54
9.1.3 证书撤销或状态信息的查询费用.....54

9.1.4 其他服务的费用.....54
9.1.5 退款策略.....54
9.2 财务责任.....54
9.3 业务信息保密.....55
9.3.1 保密信息范围.....55
9.3.2 不属于保密的信息.....55
9.3.3 保护保密信息的责任.....55
9.4 个人隐私保密.....56
9.4.1 隐私保密方案.....56
9.4.2 作为隐私处理的信息.....56
9.4.3 不被视为隐私的信息.....56
9.4.4 保护隐私的责任.....56
9.4.5 使用隐私信息的告知或同意.....56
9.4.6 依法律或行政程序的信息披露.....56
9.4.7 其他信息披露情形.....57
9.5 知识产权.....57
9.6 陈述与担保.....57
9.6.1 电子认证服务机构的陈述与担保.....57
9.6.2 注册机构的陈述与担保.....58
9.6.3 订户的陈述与担保.....58
9.6.4 依赖方的陈述与担保.....59
9.6.5 其他参与者的陈述与担保.....59
9.7 免责声明.....59
9.8 赔偿责任限制.....60
9.8.1 赔偿责任范围.....60
9.8.2 对最终实体的赔偿担保.....60
9.8.3 责任免除.....61
9.9 有限责任.....61
9.10 赔偿.....62
9.11 有效期限与终止.....62
9.11.1 有效期限.....62
9.11.2 终止.....62
9.11.3 效力的终止与保留.....63
9.12 对参与者的个别通告与沟通.....63
9.13 修订.....63
9.13.1 修订程序.....63

9.13.2 通告机制和期限.....63
9.13.3 必须修改业务规则的情形.....63
9.14 争议处理.....64
9.15 管辖法律.....64
9.16 与适用法律的符合性.....64
9.17 一般条款.....64
9.17.1 完整协议.....64
9.17.2 转让.....64
9.17.3 分割性.....64
9.17.4 强制执行.....65
9.17.5 不可抗力.....65
9.18 其他条款.....65

1 概括性描述

1.1 概述

重庆程远未来电子商务服务有限公司电子认证业务规则（以下简称《电子认证业务规则》）由重庆程远未来电子商务服务有限公司（以下简称“程远未来”），按照工业和信息化部《电子认证服务管理办法》的要求，依据《电子认证业务规则规范（试行）》制定，并报工业和信息化部备案。程远未来严格按照《中华人民共和国电子签名法》和《电子认证服务管理办法》的要求，以及相关管理规定，提供数字证书申请、颁发、存档、查询、废止等服务，并通过以 PKI 技术、数字证书应用技术为核心的应用安全解决方案，为电子商务、企业信息化构建安全、可靠的信任环境。本《电子认证业务规则》详细阐述了程远未来在实际工作和运行中所遵循的各项规范。本《电子认证业务规则》适用于程远未来及其员工、注册机构、证书申请人、订户和依赖方，各参与方必须完整地理解和执行本《电子认证业务规则》所规定的条款，并承担相应的责任和义务。

1.2 文档名称与标识

本文档名称是《程远未来电子认证业务规则》。

1.3 电子认证活动参与方及其职责

1.3.1 电子认证服务机构

电子认证服务机构是受用户信任，负责创建和分配公钥证书的权威机构，是颁发数字证书的实体。程远未来是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定，依法设立的第三方电子认证服务机构。

1.3.2 注册机构

注册机构是由电子认证服务机构授权具有下列一项或多项功能的实体：处理识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动撤销或挂起证

书，处理订户撤销或挂起其证书的请求，同意或拒绝订户更新其证书或密钥的请求。但是，RA 并不签发证书。

与程远未来建立起合同关系的第三方，如机构客户，可经程远未来授权承担 RA 的角色，并且在程远未来子 CA 下颁发证书。在不违反本 CPS 及与程远未来签署的协议的前提下，RA 可以根据其内部需求，自行制定管理流程。

程远未来除了承担 CA 角色外，同时也承担 RA 职责，订户可直接向程远未来提出证书申请。

1.3.3 订户

订户指从程远未来获得证书的个人、组织机构，即最终用户。订户通常需要同程远未来或其授权的注册机构签订合约获得证书，并承担作为证书订户的责任。

证书主体特指证书标识的实体，或者被签发证书的实体，也即证书中主体甄别名所标识的实体。

在有些情况下，证书订户和证书主体是同一个实体，如个人证书、组织机构证书；但在有些情况下，证书订户和主体不是同一实体，如设备证书的订户可以是设备所属的机构或个人，而证书主体是设备。

证书申请者指正在申请证书的证书订户或其授权者。在有些情况下，证书申请者和证书订户是同一个实体，如个人证书；但在有些情况下，他们是不同的实体，如组织机构证书的订户是该组织机构，而申请者往往是其授权人。再比如，一个组织可能为其雇员请求证书，其雇员是真正的证书订户（需要承担订户的责任），而组织机构是其授权申请者。

1.3.4 依赖方

依赖方是依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是程远未来的订户，也可以不是订户。

1.3.5 其他参与者

其他参与者指为程远未来证书服务体系提供相关服务的其他实体。

1.4 证书应用

1.4.1 适合的证书应用

因为证书标识的主体身份的不同而导致证书应用差异外，程远未来的订户证书可以广泛应用在电子政务、电子商务及其他社会化活动中，以实现身份认证、电子签名、关键数据加密等目的，同时也确保互联网上信息传递双方身份的合法性和真实性以及信息的完整性和保密性。程远未来的证书分类主要包含以下几类：

1) 个人证书：包括个人身份证书、个人邮件证书等，可用于需要区分、标识、鉴别个人身份的场合，还可用于数据加解密和信息签名，包括订单、合同签名，以实现信息保密，提供信息源发性证明、完整性保障和抗抵赖。
2) 机构证书：包括机构单位证书、机构部门证书、机构职位证书和机构职员证书，可用于需要区分、标识、鉴别机构身份的场合，还可用于数据加解密和信息签名，包括订单、合同签名，以实现信息保密，提供信息源发性证明、完整性保障和抗抵赖。
3) 设备证书：设备证书用于标识终端、服务器、运营设备，还可用于数据加解密和信息签名，以实现信息保密，及提供信息源发性证明、完整性保障。

1.4.2 受限的证书应用

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，将不受程远未来的保护。

任何未经程远未来认可的证书应用都将不受程远未来的保护。

1.4.3 禁止的证书应用

程远未来签发的证书在如下情况被禁止使用：

1) 禁止在违反国家法律、法规的情况下使用本机构颁发的数字证书。
2) 禁止用于危险环境中的控制设备或应用系统。例如，航天航空导航或通讯系统，武器控制系统，以及其它故障可能导致人员死亡、伤害或严重破坏环境的情况。

1.5 策略管理

1.5.1 策略文档管理机构

本《电子认证业务规则》的管理机构是程远未来安全策略委员会。由程远未来安全策略委员会负责本《电子认证业务规则》的制订、发布、更新等事宜。

本《电子认证业务规则》由重庆程远未来电子商务服务有限公司拥有完全版权。

1.5.2 联系人

本《电子认证业务规则》在程远未来网站发布，对具体个人不另行通知。

网站地址：http://www.ifutureca.com

电子邮箱：cps@ifutureca.com

联系地址:重庆市渝北区人和街道镜泊中路 5 号远大印务 1 栋 1 层(401121)

电话号码：023-63063149

传真号码：023-63061694

1.5.3 决定 CPS 符合策略的机构

本《电子认证业务规则》由程远未来安全策略委员会组织制定，报程远未来安全策略委员会批准实行。

1.5.4 CPS 批准程序

本《电子认证业务规则》由程远未来安全策略委员会，组织 CPS 编写小组。编写小组完成编写 CPS 草案后，由程远未来安全策略委员会组织对 CPS 草案进行初步评审。初步评审后，将 CPS 评审稿提交程远未来安全策略委员会审批。经程远未来安全策略委员会审批通过后，在程远未来的网站上对外公布。

根据《电子认证服务管理办法》规定，本 CPS 经程远未来安全策略委员会审批通过后，从对外公布之日起三十日之内向工业和信息化部备案。

1.5.5 CPS 修订

程远未来会根据国家的政策法规、所适用的证书策略、技术要求和业务发展情况修订 CPS，CPS 编写小组根据相关的情况拟定 CPS 修订建议，提交安全策略委员会审批，经该委员会批准后，在程远未来的网站上对外公布。

修订后的 CPS，从对外公布之日起三十日之内向工业和信息化部备案。

1.6 定义和缩写

下列定义适用于本《电子认证业务规则》：

- 公开密钥基础设施（PKI）Public Key Infrastructure

公钥基础设施是一套由硬件、软件、人员、策略和流程构成的，用于生成、管理、分发、使用、存储和撤销数字证书的，利用公钥技术提供安全服务的基础设施。

- 电子认证服务机构（CA）Certification Authority

受用户信任，负责创建和分配公钥证书的权威机构。

- 注册机构（RA）Registration Authority

具有下列一项或多项功能的实体：识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动撤销或挂起证书，处理订户撤销或挂起其证书的请求，同意或拒绝订户更新其证书或密钥的请求。但是，RA 并不签发证书。

- 订户 Subscriber

订户是与电子认证服务机构签订协议，接受电子认证服务机构提供的服务的

实体。订户应对证书对应的私钥使用负有法律责任。

- 证书主体 Subject

证书主体是证书中的“主体”（Subject）项指明的、持有与证书中载明公钥相对应之私钥的实体。证书主体可以是订户自己，也可以是订户全权控制的设备、账号、域名、IP 地址等。当订户是机构时，证书主体还可以是该机构的下属机构、部门、职员和设备等。

- 证书申请者（也称作证书申请人）Certificate Applicant

证书申请者是指向电子认证服务机构申请证书的个人或机构。证书申请成功后，证书申请者即为订户。

- 证书申请递交人 Certificate Application Deliverer

指向电子认证服务机构或注册机构递交证书申请的自然人，可以是订户或者订户的合法代表。

- 证书策略（CP）Certification Policy

是关于电子认证服务机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

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

CPS 是电子认证服务机构在证书生命周期管理过程中所采纳的业务实践的声明。CPS 是对 CP 所宣称内容的一种解释性和支持性文档。

- 密码模块 Cryptography Module

具有安全边界的用于进行密码相关的存储和计算操作的软件或硬件组合。

- 激活数据 Activation Data

用于使密码模块进入可操作状态的数据，可以是口令、生物特征等。

- 依赖方协议 Relying Party Agreement

电子认证服务机构在《电子认证业务规则》或单独载明的与依赖方之间的协议中，规定双方在证书使用和管理过程中所承担的责任和义务。

- 订户协议 Subscriber Agreement

电子认证服务机构与订户所签署的协议，规定了双方在证书使用和管理过程中所承担的责任和义务。

- 数字证书 Digital Certificate

是电子认证服务提供者签发的用以证明证书持有人的电子签名、身份、资格及其他有关信息的电子文件。证书包含有公开密钥拥有者的信息、公开密钥、签名算法、密钥用途和 CA 的数字签名。

- 甄别名（DN，也被称作可辨识名）Distinguished Name

用于标识证书颁发机构和证书主体名称的序列，一般包括国家名称、省名、地理位置、机构名、机构单元名称和通用名称。

- 对象标识符（OID）Object Identifier

对象标识符是一串数字，可以唯一地标识一个对象（例如密码算法、证书策略等）。

- 证书撤销列表（CRL）Certificate Revocation List

证书撤销列表是由电子认证服务机构维护的，包含由于各种原因（例如私钥泄漏、证书中的信息发生改变）在有效期内被撤销的证书的列表，也称证书黑名单。

- CA 撤销列表（ARL）Authority Revocation List

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

- 证书信任链 Certificate Chain

证书信任链是一个用于证书验证的有序证书序列，它包含一个终端订户证书和若干电子认证服务机构证书，证书信任链起始于根证书，终止于终端订户证书。

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

为订户或依赖方提供在线证书状态查询的协议。

- 目录服务（LDAP）Lightweight Directory Access Protocol

轻量级目录访问协议，通常也指符合轻量级目录访问协议的目录服务系统。

- 私钥（电子签名制作数据）Private Key

指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。私钥是经由数字运算产生的密钥，用于制作电子签名数据，亦可依据其运算方式，就相对应的公开密钥加密的文件或信息予以解密。

- 公钥（电子签名验证数据）Public Key

公钥是经由数字运算产生的密钥，用于解密电子签名，确认电子签名人的身

份及电子签名的真实性。公钥可以公开，一般标示于在线数据库、存储库或其他公共目录中，使任何希望得到公钥的人都能得到。

- 会话密钥 Session Key

在一次会话中有效地对消息进行加密的密钥，通常为对称算法密钥。

2 信息发布与信息管理

2.1 认证信息的发布

程远未来 CA 证书、CRL、证书策略、电子认证业务规则，可从程远未来公司网站获取。

用户证书可从程远未来的目录服务或证书服务站点查询获取。已被撤销的证书信息可从目录服务或 CRL 站点查询获取。证书的状态（有效、撤销）可通过 OCSP 查询获取。

实际的应用场景中，用户证书和证书状态查询获取方式可以是以上方式的全部，也可以是其中之一，视具体的安全需求而定。

2.2 发布时间或频率

《程远未来电子认证业务规则》的变更，应在审批通过之日起十天内发布。一经发布，即时生效。对数字证书的订户及证书申请人均具备约束力，对具体个人不另行通知。

证书的发布：在证书签发时，程远未来自动将该证书发布到目录服务。

CRL 的发布：CRL 的发布时间和频率详见§4.9.7。

OCSP 对证书状态的查询是及时的。

2.3 信息库访问控制

对于公开发布的 CP、CPS 和 CA 证书等公开信息，本 CA 机构允许公众自行通过网站进行查询和访问。

§2.1 中所说的用户证书的查询、CRL 的下载是公开的、没有限制的。程远

未来通过网络安全防护、系统安全设计、安全管理制度确保这些信息只有授权人员才能修改。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

根据证书类别的不同，签发的证书主体名字可能是证书订户的真实名称、域名、设备名称等，命名符合 X.501 定义的甄别名规范。

3.1.2 对名称意义化的要求

订户证书的主体甄别名（DN）必须具有一定的代表意义。

个人证书主体甄别名中的通用名通常是个人的真实姓名，甄别名应包含其他能唯一标识用户身份的信息，如个人身份证号码等，它作为标识订户的关键信息被鉴别和认证。出于个人隐私保护的考虑，证书中的身份证号码可以是加密的。

机构单位证书主体甄别名的通用名通常是组织机构的名称，甄别名应包含其他能唯一标识该机构的信息，如统一社会信用代码、组织机构代码等，它作为标识订户的主要信息同其他信息一起被鉴别和认证。

设备证书主体甄别名中的通用名通常是该组织机构的设备名，如域名、IP 地址等，它作为标识订户的主要信息同其他信息（如组织机构名称）一起被鉴别和认证。

3.1.3 订户的匿名或伪名

使用匿名的订户提交的证书申请材料不符合程远未来的审核要求，将无法通过审核，也无法获得证书和服务。

使用伪名或伪造材料申请的证书无效，一经证实立即予以撤销。

3.1.4 理解不同名称形式的规则

依 X.501 甄别名命名规则解释。

3.1.5 名称的唯一性

程远未来签发给某个实体的证书，其主体甄别名，在该证书签发 CA 信任域内是唯一的，其中的例外是签发双证书时（一个签名证书、一个加密证书），属于同一实体的两个证书具有同样的主体甄别名，但证书的密钥用法扩展项不同。

3.1.6 商标的承认、鉴别和角色

证书申请者不应在其证书申请中使用侵害他人知识产权的名称，但程远未来并不决定证书申请者是否具有相关知识产权，也无需判断、裁决或解决任何关于域名、名称、商标、服务标的争端问题。当出现此类争端时，程远未来有权拒绝或挂起证书申请，直到争端得到有效解决。

3.2 初始身份确认

3.2.1 证明持有私钥的方法

如果证书私钥在订户一端生成的，证书申请者应证明持有与所要注册公钥相对应的私钥。在程远未来证书服务体系中，通过证书请求中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。私钥先在用户端生成，证书请求信息中包含用私钥进行的数字签名，CA 用其对应的公钥来验证这个签名。

如果密钥对是程远未来或其授权的注册机构为订户生成的，则不需要进行上述证明，但需要以安全的方式送达给证书申请人。

程远未来要求证书申请人妥善保管自己的私钥，证书申请人视作其私钥的唯一持有者。

3.2.2 机构身份的鉴别

签发机构证书、设备证书时，程远未来对组织机构进行身份鉴别，鉴别包括

如下两方面内容：

1) 确认组织机构是确实存在的、合法的实体。机构订户需要向程远未来或其授权的注册机构提交政府签发的组织机构成立的有效文件，如营业执照、组织机构代码证等合法证件的副本（如复印件或电子形式的扫描件），程远未来通过权威的第三方数据库确认其真实性。
2) 确认该组织机构知晓并授权证书申请，即代表组织机构提交证书申请的人是经过授权的。确认的方式可以是：
   a) 使用从网络或其它常规途径获取验证电话号码，进行电话验证，获得组织机构有关申请及授权事宜的确认；
   b) 由该机构提供加盖公章的授权书、传真确认；
   c) 验证机构申请者知晓或拥有通常只有真正的申请者才知晓或拥有的秘密。如申请者使用其对公账号支付证书申请费用，或者程远未来或其授权的注册机构向申请者的对公账号进行小额打款，申请者能够准确的提供打款金额等；
   d) 功能等同的其他安全可靠方式。
3) 按照§3.2.3，对机构证书申请递交人进行个人身份鉴别。

用于办理机构业务的机构职员证书，按机构证书进行鉴别。机构职员个人直接向程远未来或其授权的注册机构提交申请的，还需要通过电话、该机构提供的加盖公章的信函、传真等方式确认申请人是属于该组织机构的员工。签发属于组织机构的设备证书时，程远未来或其授权的注册机构除了对组织机构进行身份鉴别，还要求确认组织机构知晓并授权设备证书申请。对于具有公共资源属性的服务器证书，需要确认组织机构对域名有所有权或使用权。确认的方式可以是，通过域名注册商确认域名所有者信息。

当程远未来对外向有关机构（如注册机构或其他授权机构）签发与运营有关的设备证书时，将通过电话或书面形式（包括传真、信函），向该机构的有关责任人确认设备证书申请者来自该机构，且有关申请获得了授权。

3.2.3 个人身份的鉴别

个人订户申请个人证书时，应向程远未来或者程远未来的注册机构提供真实有效的个人身份信息。程远未来首先对申请材料进行初步完整性检查，其次对证书申请者的身份信息进行鉴别，其鉴别分为两个方面：

1) 确认证书申请者提交的个人身份信息真实存在且正确。

个人订户需要向程远未来或其授权的注册机构提交其本人真实身份证件副本（如复印件或电子形式的扫描件），程远未来采用权威的身份证实服务的数据库中的信息对该身份信息进行查验，如公安部门提供的个人身份数据库、主流的信用机构或其他可靠的信息源等。

2) 验证证书申请者是身份信息所对应的本人。验证的方式包括但不限于：

- 面对面验证申请者身份证件真伪，并确认申请者是否为证件所有者本人；
- 验证申请者知晓或拥有通常只有真正的申请者才知晓或拥有的秘密，如银行账户信息、银行预留手机号的短信验证等；
- 通过可靠的科技手段验证申请者是否为申请者本人，如人脸识别、指纹识别等；
- 功能等同的其他安全可靠方式。

证书申请者委托他人申请的，需要出示证书申请者的授权文书，并对授权代表进行同等方式个人身份鉴别。

签发属于个人的设备证书时，程远未来或其授权的注册机构除了对个人进行身份鉴别，还要求确认个人知晓并授权设备证书申请。对于具有公共资源属性的服务器证书，需要确认个人对域名有所有权或使用权。确认的方式可以是，通过域名注册商确认域名所有者信息。

3.2.4 没有验证的订户信息

程远未来不对下列订户信息进行验证：组织机构部门（OU）、机构所设职位、证书中指明不验证的其他信息。

3.2.5 授权确认

当证书申请递交人代表组织机构申请数字证书，应出示足够的证明信息以证明申请人获得了组织机构的授权。证明信息可以是组织机构在申请表上加盖单位公章，组织机构出具独立的授权文件并加盖公章等。程远未来有责任对授权进行确认，确认的方式包括电话、书面形式（包括信函、传真）等。

3.2.6 互操作准则

互操作可能是交叉认证、单身交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各自认证策略的 CA 中心之间建立相互信任关系，从而使双方的订户可以实现互相认证。程远未来将根据业务需要，在遵循本《电子认证业务规则》的各项控制要求的基础上，与程远未来证书服务体系中未涉及的其他电子认证服务机构建立交叉认证关系。但交叉认证并不表示程远未来批准了或赋予了其他 CA 中心或电子认证服务机构的权力。

3.3 密钥更新请求的身份标识与鉴别

证书密钥更新的情形在§4.7.1 进行约定。

3.3.1 常规密钥更新的标识与鉴别

订户在证书有效期内、且证书未被撤销的情况下提出密钥更新请求，视为常规密钥更新请求。在常规密钥更新时，程远未来或其授权的注册机构应对订户进行身份鉴别。鉴别方式有：

- 订户使用当前有效私钥对包含新公钥的密钥更新请求进行签名；
- 质询短语、预留手机短信验证码或其他同等安全验证手段。

质询短语是订户在申请证书时留下的用于身份鉴别的短语。利用质询短语进行鉴别时，订户应正确提供该短语的内容，并能正确提供部分其他信息。若采用私钥签名的方式进行鉴别，订户应使用现有私钥对更新请求进行签名，更新请求中包含正确的部分登记信息。电子认证服务机构应对订户的签名和更新请求内所包含的订户信息进行验证。

3.3.2 撤销后密钥更新的标识与鉴别

证书撤销后的密钥更新等同于订户重新申请证书，其要求详见§3.2.2 机构身份的鉴别，§3.2.3 个人身份的鉴别。

3.4 撤销请求的标识与鉴别

订户本人撤销时的身份标识和鉴别使用原始身份验证相同的流程，详见§3.2.2 机构身份的鉴别，§3.2.3 个人身份的鉴别。

订户主动发起的证书撤销申请，程远未来或其授权的注册机构应对证书撤销申请人进行身份鉴别，确认撤销申请人是订户本人，鉴别方式包括：

- 使用与初始身份验证相同的流程，详见§3.2.2 机构身份的鉴别，§3.2.3 个人身份的鉴别。
- 质询短语、预留手机短信验证码或其他同等安全验证手段。

如果是因为订户没有履行本《电子认证业务规则》所规定的义务，由程远未来或其授权的注册机构申请撤销订户的证书时，不需要对订户身份进行标识和鉴别。

由司法机关依法提出的证书撤销，电子认证服务机构将直接以司法机关书面撤销请求文件作为依据，不再进行其他方式的鉴别。

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

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

- 个人证书由申请人本人或其授权代表申请。
- 组织机构申请机构证书时，由机构授权人员申请。

- 属于个人的设备证书由拥有者本人或其授权代表申请。属于机构的设备证书由所属机构的授权人员申请。

4.1.2 申请过程与责任

证书申请者可在线申请或到程远未来或其授权的注册机构现场办理各类证书业务。申请者在线申请所提交的信息应与现场办理所提交的信息基本一致。

对于机构证书，注册时申请者须正确填写以下信息：

- 机构的真实身份标识信息，如机构法定名称、统一社会信用代码、组织机构代码等；
- 机构授权的申请人信息，如姓名、身份证号码、电话、邮件地址等。

对于个人证书，注册时申请者须正确填写以下信息：

- 个人的真实身份标识信息，如个人真实姓名、身份证号码、实名登记的电话号码、所属机构（若需要）等；
- 其他信息，如邮件地址等。

对于服务器证书和设备证书，注册时申请者须正确填写以下信息：

- 服务器主机名、域名、IP 地址、或设备名称、及所有者信息等；
- 申请人信息，如姓名、电话、邮件地址等。
- 现场申请审核过程中信息录入和信息审核由不同的操作人员完成，采用双人控制。
- 在线申请信息录入由证书申请人完成，信息审核由审核人员或鉴证系统完成，两个过程采用不同人员或鉴证系统控制。

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

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

程远未来或其授权的注册机构按照本《电子认证业务规则》所规定的身份鉴

别流程对申请人的身份进行识别与鉴别。具体的鉴别流程详见§3.2.2 机构身份的鉴别、§3.2.3 个人身份的鉴别。

4.2.2 证书申请批准和拒绝

程远未来或其授权的注册机构根据本《电子认证业务规则》§3.2.2 和§3.2.3 所规定的身份鉴别流程对证书申请者身份进行识别与鉴别后，根据鉴别结果决定批准或拒绝证书申请。

如果证书申请者通过本《电子认证业务规则》所规定的身份鉴别流程、鉴别结果为合格，并且证书申请者履行了其他应尽责任（如付款等），程远未来或其授权的注册机构将批准证书申请，为证书申请者制作并颁发数字证书。

如果发生下列情形之一，程远未来或其授权的注册机构应拒绝证书申请。

- 证书申请者未能通过身份鉴别；
- 证书申请者不能提供需要的补充文件或没有在指定的时间内响应程远未来或其授权的注册机构的通知；
- 未收到或确认无法收到申请证书所需要缴纳的费用；

程远未来或其授权的注册机构拒绝申请人证书申请的，应及时通知证书申请者，并提供失败的原因（法律禁止的除外）。

4.2.3 处理证书申请的时限

程远未来或授权的注册机构应做出合理努力来尽快确认证书申请信息。在申请者提交资料齐全且符合要求的情况下，处理证书申请的时间不超过两个工作日。

4.3 证书签发

4.3.1 证书签发过程中电子认证服务机构的行为

作为证书认证系统的运营者，程远未来既是一个电子认证服务机构，同时也承担了注册机构的职能。

证书现场办理时，具有权限的业务操作员负责证书申请的录入工作并提交证

书申请后，具有权限的业务审核员将审核批准或拒绝证书请求。批准的信息将会发送到程远未来的 CA 系统，CA 系统签发证书并返回给系统供证书申请者下载。

证书在线办理时，证书申请信息由订户提交或来自业务系统，程远未来或其授权的注册机构按照§3.2.2、§3.2.3 的要求对其身份进行人工或自动的鉴别验证，并根据结果批准或拒绝申请。

4.3.2 电子认证服务机构对订户的通告

无论是拒绝还是批准订户的证书申请，程远未来及其授权的注册机构有义务告知订户申请结果。可通过面对面、电话、电子邮件、短信或其他程远未来认为安全可行的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

对于由注册机构替证书订户产生证书请求、证书密钥对、下载证书的情形，则订户通过面对面的方式从程远未来或其授权的注册机构接受载有证书和私钥的介质的行为，即表明了用户接受了证书；或者当订户通过其他方式，如邮件快递，接收载有证书和私钥的介质后，在订户收到证书之后且在规定时限内未对证书或证书内容提出异议，即表明订户接受了证书。

对于订户自行下载证书的情形，订户通过特定站点将证书下载到本地数字证书存放介质。系统记录订户下载了证书即表明订户接受了证书。

4.4.2 电子认证服务机构对证书的发布

除非与证书订户间有特别的约定，程远未来在签发完证书后，会将证书发布到目录服务器中。程远未来采用主、从目录服务器结构来发布所签发的证书。签发完成的数据直接写入主目录服务器中，然后通过主从映射，将主目录服务器的数据自动发布到从目录服务器中，供订户和依赖方查询和下载。

4.4.3 电子认证服务机构在颁发证书时对其他实体的通告

对于程远未来签发的证书，程远未来及其授权的注册机构不通知其他实体。其他实体可以通过目录服务自行查询。

4.5 密钥对和证书的使用

密钥对和证书不应用于其规定的、批准的用途之外的目的，否则其应用是不受相关法律和程远未来策略保障的。

4.5.1 订户私钥和证书的使用

订户在接受了程远未来所签发的证书后，均视为已经同意遵守与程远未来、依赖方有关的权利和义务的条款。订户私钥的使用应符合证书中“密钥用途”(Key Usage）和“增强密钥用途”（Extended Key Usage）的要求。订户接受到数字证书，应妥善保管其证书对应的私钥，避免他人未经本人授权而使用本人证书情形的发生；订户只能在指定的应用范围内使用私钥和证书，否则其应用是不受保障的。订户只有在接受了相关证书之后才能使用对应的私钥，并且在证书到期或被撤销之后，订户必须停止使用该证书对应的私钥。

4.5.2 依赖方对公钥和证书的使用

依赖方信任证书的前提是同意依赖方协议中的条款。依赖方应依据证书使用的环境和条件判断证书是否可以信任。如果依赖方需要电子认证服务机构提供额外的保障，依赖方应在确认可以获得这些保障之后信任相应的证书。

在信任证书之前，依赖方应独立的进行如下评估：

- 证书适用于当前的应用场景，并确定证书的使用不违背本证书策略的要求；
- 证书的使用不违背证书中“密钥用途”（Key Usage）和“增强密钥用途”（Extended Key Usage）的规定；
- 证书及其证书信任链中所有电子认证服务机构证书的证书状态是合适的。当证书信任链中的某个证书有被撤销的情况时，依赖方有责任调查

上述证书撤销前，订户证书对应私钥所做的签名是否可以信任，并独立承担相应的风险。

依赖方应利用合适的软硬件来执行数字签名验证和数字证书验证，验证证书的有效性包括三个方面的内容：

1) 用程远未来的证书验证证书中的签名，确认该证书是程远未来签发的，并且证书的内容没有被篡改。
2) 检验证书的有效期，确认该证书在有效期之内。
3) 查询证书状态，确认该证书没有被撤销。

在验证电子签名时，依赖方应准确知道什么数据已被签名。

4.6 证书更新

证书更新是指基于原有的证书信息，为订户签发一张新的证书。新证书的序列号和有效期将发生改变，证书密钥是否更新视具体的安全需求而定，其他信息如签发者、证书主体甄别名、证书用途等均不改变。

4.6.1 证书更新的情形

1) 订户证书到期，需要延期的情形；

证书上都有明确的证书有效期，表明该证书的起始日期与截止日期。订户应当在证书有效期到期前三个月，向程远未来或其授权的注册机构申请更新证书。对于过期的证书更新申请，程远未来或其授权的注册机构将根据实际的安全需求决定是否允许更新。证书撤销后，将无法进行更新，只能按照初始流程重新申请证书。在证书密钥使用年限内，证书更新一般只延长有效期，不更新密钥对。

2) 因为安全需求，需要密钥更新的情形。如订户的证书介质损坏或遗失，需要补发证书。

4.6.2 请求证书更新的实体

订户可以请求证书更新。订户包括持有程远未来签发的个人、机构及设备等各类证书的证书持有人。

4.6.3 证书更新请求的处理

程远未来或其授权的注册机构，应对请求证书更新的订户身份进行鉴别，确认更新请求是证书订户或订户授权代表提出的。

订户应使用拟被更新的证书对应的私钥对更新请求进行签名。如果订户以前提交的身份证明材料已过期，程远未来或其授权的注册机构需要重新对订户进行初始身份鉴别，鉴别要求同§3.2.2、§3.2.3；如果身份证明材料未过期，则证书更新申请人无需重新提交有关身份证明文件，但程远未来或其授权的注册机构仍会通过权威数据库验证有关材料是否有效。

对于订户不能提供拟被更新证书对应私钥签名的，应按初始证书申请流程处理，详见§4.2。

4.6.4 颁发新证书时对订户的通告

同§4.3.2。

4.6.5 构成接受更新证书的行为

同§4.4.1。

4.6.6 电子认证服务机构对更新证书的发布

同§4.4.2。

4.6.7 电子认证服务机构在颁发证书时对其他实体的通告

同§4.4.3。

4.7 证书密钥更新

证书密钥更新指的是订户更换证书密钥对的证书更新行为。证书密钥包括签名证书密钥和加密证书密钥。

4.7.1 证书密钥更新的情形

a）订户证书密钥遗失或遭到损坏；

b）订户证实或怀疑其证书密钥不安全；

c）其他安全需求，如安全策略对证书密钥使用年限的要求。

出现上述情况，除非订户特别要求，程远未来一般建议订户不进行证书密钥更新操作，而是撤销原有证书，重新进行证书申请。

4.7.2 请求证书密钥更新的实体

同§4.6.2。

4.7.3 证书密钥更新请求的处理

同§4.6.3。

4.7.4 颁发新证书对订户的通告

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

同§4.4.2。

4.7.7 电子认证服务机构在颁发证书时对其他实体的通告

同§4.4.3。

4.8 证书变更

4.8.1 证书变更的情形

证书变更是指订户的证书信息发生变更，需要重新签发证书的情形。如果订户证书信息以外的信息发生改变，如联系地址、电话号码等，可以向程远未来提出注册信息修改，无需证书变更。

4.8.2 请求证书变更的实体

请求证书变更的实体为证书订户。

4.8.3 证书变更请求的处理

证书变更需要先对原证书进行撤销处理（同§4.9.3），然后按照初次申证书过程进行处理（同§4.2）。

4.8.4 颁发新证书时对订户的通告

同§4.3.2。

4.8.5 构成接受变更证书的行为

同§4.4.1。

4.8.6 电子认证服务机构对变更证书的发布

同§4.4.2。

4.8.7 电子认证服务机构对其他实体的通告

同§4.4.3。

4.9 证书撤销和挂起

4.9.1 证书撤销的情形

1) 发生下列情形之一的，订户应当申请撤销数字证书：
   a) 数字证书私钥泄露；
   b) 数字证书中的信息发生重大变更；
   c) 认为本人不能实际履行电子认证业务规则。
2) 发生下列情形之一的，程远未来或其授权的注册机构可以撤销其签发的数字证书：
   a) 订户申请撤销数字证书；
   b) 订户提供的信息不真实；
   c) 订户没有履行双方合同规定的义务；
   d) 法律、行政法规规定的其他情形。

4.9.2 请求证书撤销的实体

根据不同的情况，订户、程远未来、注册机构、司法机关等公共权力部门可以请求撤销最终用户证书。

4.9.3 撤销请求的流程

当程远未来或其授权的注册机构有充分的理由相信需要撤销订户的证书时，程远未来或其授权的注册机构的有关人员可以通过内部确定的流程提请撤销证书。在证书撤销后，程远未来或其授权的注册机构将通过适当的方式，包括邮件、传真、短信等，通知订户证书已被撤销及被撤销的理由。

订户主动要求撤销自己的证书的，应提供有效身份证明文件及证书撤销申请文件，并接受证书撤销申请的有关条款，同意承担相应的责任。机构订户撤销证书应由其授权代表提出申请。

订户可通过面对面、电子邮件、传真、特快专递等可靠的方式向程远未来或其授权注册机构提出证书撤销申请。收到订户的撤销申请材料后，程远未来或其

授权的注册机构将确认订户需撤销的证书是否为程远未来所签发，证书是否在有效期内，撤销理由材料和撤销理由是否属实，若均通过则对证书进行撤销。

4.9.4 撤销请求宽限期

在订户主动要求撤销的情形下，订户一旦发现需要撤销证书，应及时向程远未来及其注册机构提出撤销请求。从发现需要撤销证书到向程远未来或其授权的注册机构提出撤销请求的时间间隔的要求如下：

- 对于个人证书不能超过 8 小时。
- 对于机构证书和设备证书不能超过 4 小时。

4.9.5 电子认证服务机构处理撤销请求的时限

程远未来或其授权的注册机构从接到撤销请求到完成处理请求的时间如下:

- 对于个人证书不能超过 8 小时。
- 对于机构证书和设备证书不能超过 4 小时。

4.9.6 依赖方检查证书撤销的要求

依赖方在信任证书之前，必须使用以下方法之一进行所依赖证书的状态查询：

- CRL 查询：利用证书中标识的 CRL 地址，通过目录服务器提供的查询系统，查询并下载 CRL 到本地，进行证书状态的检验。
- 在线证书状态查询（OCSP）：服务系统接受证书状态查询请求，从目录服务器中查询证书的状态，查询结果经过签名后，返回给请求者。
- 与电子认证服务机构或注册机构约定的其他在线证书查询方式。

注意：依赖方要验证 CRL 的可靠性和完整性，确保是经程远未来发布并且签名的。

4.9.7 CRL 的签发频率

程远未来采用实时或定期的方式发布 CRL。

ARL 每年签发一次，或者当 CA 证书需要撤销时签发 ARL。

订户证书的 CRL 签发频率一般为 24 小时或当证书撤销时立即签发。对于特殊的客户，程远未来可为其专门定制证书撤销列表的更新频率。程远未来对每个证书签发 CA 发布一个证书撤销列表，发布该 CA 签发的证书中已撤销了的证书。

4.9.8 CRL 发布的最长滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.9.9 证书状态查询的可用性

程远未来提供证书状态在线查询服务（OCSP），服务 7*24 小时可用。

程远未来提供的证书撤销列表查询服务，7*24 小时可用。

4.9.10 撤销信息的其他发布形式

除了通过 LDAP 目录服务发布 CRL，或通过 OCSP 服务器提供证书状态查询外，程远未来所发布的 CRL 也可通过程远未来的相关服务网站获得。

4.9.11 对密钥遭受安全威胁的特别处理要求

如果电子认证服务机构发现或有理由相信其私钥泄露，应立即上报电子认证服务管理部门，并尽可能及时的通知所有订户、潜在的证书依赖方和其他参与方。

4.9.12 证书挂起

程远未来目前暂不提供此业务。

4.10 证书状态服务

程远未来通过网站 CRL、OCSP、LDAP 提供证书状态服务。

对于被撤销证书，其状态将同时在 CRL、OCSP 反映。

4.10.1 操作特点

程远未来提供的证书状态查询以网络服务的形式：

- CRL 采用 HTTP 或 LDAP 方式提供；
- OCSP 符合 RFC2560，反映证书的当前状态；
- 证书目录 LDAP 符合 LDAP V3（RFC3377，2251-2256，2829-2830）。

4.10.2 服务可用性

程远未来提供 7*24 小时的证书状态查询服务。即在网络允许的情况下，订户能够实时获得证书状态查询服务。

4.10.3 可选特征

根据请求者的要求，电子认证服务机构可以提供指定证书的撤销通知服务。

4.11 订购结束

订购结束是指当证书有效期满或证书撤销后，该证书的服务时间结束。

订购结束包含以下两种情况：

1) 证书有效期满，订户不再进行证书更新、证书变更或者证书密钥更新，订户可以终止订购；
2) 在证书有效期内证书被撤销后，且订户没有进行证书变更或者证书密钥更新，即订购结束。

4.12 密钥托管与恢复

程远未来依国家密码管理部门的相关规定，提供加密证书密钥的集中产生、保存和恢复。

4.12.1 密钥托管与恢复的策略与行为

程远未来的 CA 签名密钥由程远未来数据机房自行保管。

程远未来订户的签名密钥托管需满足《中华人民共和国电子签名法》可靠电子签名的要求。

订户加密证书密钥对可以由密钥管理中心系统集中安全产生和保存，密钥恢复是一种严格受控的过程，只有在如下情况下才允许进行密钥恢复：

- 证书持有者提出申请；
- 国家执法、司法机构因执法、司法的需要；
- 国家其他管理部门管理需要。

密钥恢复只有在必须的情况下才进行，并且申请要提出充分的理由和提供有关文件、材料。

4.12.2 会话密钥的封装与恢复的策略与行为

会话密钥是指用户在使用证书建立加密通道时临时生成的加密密钥，该密钥由应用环境来决定使用，程远未来不对其进行保存和恢复。

5 电子认证服务机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

程远未来机房位于重庆市渝北区人和街道镜泊中路 5 号远大印务 1 栋 1 层，实行分区域访问的安全管理。程远未来的功能区域划分为四个区域，分别是：公共区、服务区、管理区和核心区。程远未来 CA 密钥的存储和使用设备放置在核心区，并进行了电子屏蔽。

程远未来的建筑物和机房建设按照下列标准实施：

1) GB2887-2000《电子计算机场地通用规范》；
2) GB9361《计算机站场地安全要求》；
3) GM/T 0018-2012《密码设备应用接口规范》；
4) GB50174-2008《电子信息系统机房设计规范》；
5) GB30003-93《电子计算机机房施工及验收规范》；

6）GB50222-95《建筑内部装修设计防火规范》；

7）GB50116-98《火灾自动报警系统设计规范》；

8）GB50057-94《建筑物防雷设计规范》；

9）GB5054-95《低压配电设计规范》；

10）GB/J19-87《采暖通风与空气调节设计规范》；

11）SJ/T10796-1996《计算机机房用活动地板技术条件》；

12）YD/T754-95《通讯机房静电防护通则》；

13）BMB3-1999《处理涉密信息的电磁屏蔽室的技术要求和测试方法》。

5.1.2 物理访问

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

物理访问控制包括如下几个方面：

- 门禁系统：控制各层门的进出。工作人员需使用身份识别卡结合指纹鉴定才能进出，进出每一道门应有时间记录和信息提示。机房安装了动环监控系统，对门禁系统进行监控，实时读取门禁记录的资料，并对门禁系统设置权限。
- 报警系统：门禁系统有门开超时报警，当门打开时间超过 30 秒钟或者门打开后 30 秒内没有关好，门禁自动发出警告提醒工作人员及时把门关好，每月对门禁记录进行整理归档。
- 监控系统：根据机房动力环境保安监控系统的要求，机房环境监控系统包括子系统有：配电检测子系统、UPS 检测子系统、空调设备检测子系统、温湿度检测子系统、漏水监测子系统、消防子系统、门禁子系统、图像监控子系统。

程远未来的四个功能区域按照安全级别逐级分层，当人员从一个区域进入安全级别较高的区域时，需进行相应的访问控制。

公共区为程远未来的办公场地，大门处设有电子门禁系统，使用指纹或人脸

识别验证方式进入。

服务区为客户服务和业务办理区域，位于公共区域内，设有电子门禁系统，授权人员采用指纹和 IC 卡验证方式进入。

管理区为程远未来机房监控和电子认证服务系统配置管理的区域，包括过道、走廊、监控室、管理室和配电室。动力环境监控系统位于监控室，CA 和 RA 的配置管理终端位于管理室。授权人员需采用双因素认证方式（指纹和 IC 卡）进入管理区，访客需验证身份并登记后方可进入，且需要有授权人员的陪同。监控室、管理室和配电室又分别设有电子门禁系统，授权人员需要再次通过双因素认证后才能进入。

进入核心区需要先通过管理区访问控制，核心区包括标准机房、CA 屏蔽机房和 KM 屏蔽机房。授权人员需要通过双人双因素认证（指纹和 IC 卡）后才能进入。所有网络设备和服务器存放于核心区，所有进出屏蔽机房的线路都需经过滤波处理或者将电磁信号转换为光信号，将电磁泄漏减到最低。

5.1.3 电力与空调

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统。

机房采用两路市电电源，电源线接至市电配电柜。在标准机房配备一台独立的市电配电柜和 UPS 配电柜，管理标准机房的用电设备供电，在屏蔽机房配备一台市电和 UPS 一体柜，管理屏蔽区域的用电设备供电。机房采用英威腾公司的 UPS 一台，组成不间断供电系统，供给机房设备用电，每回路容量按设备实际用电量进行施工，并留有一定的余量。UPS 灯跟市电灯独立工作，保证在市电灯供电出现问题时，UPS 灯也能正常启动工作。停电时，UPS 照明系统由 UPS 自动供电。

程远未来具有新风/空调系统控制运营设施中的温度和湿度环境。根据机房环境及设计规范要求，标准机房和屏蔽机房，均设置了空气调节系统。空调系统使用精密空调，并采用独立空调作为备份。其组成包括精密空调、通风管路、新风系统。程远未来的要求参照电信设施管理的规定，而且每年对物理系统的安全性进行检查。

5.1.4 水患防治

机房位于五层楼房的一层，楼层上方无水源，机房内无渗水、漏水现象。机房具有漏水监测子系统，监控系统上均采用电子地图形式显示漏水的具体位置，方便机房管理人员迅速查找有漏水的地方。当感应线缆感应到某处有漏水事件发生时系统将即刻响应，弹出相应的报警窗口，可从监控主机上的电子地图上线缆的颜色变化来判断报警的发生，通过具体的数值显示来确定报警位置。在以上报警方式发生的同时，现场值班室还将通过多媒体声音报警并自动拨号通知相关人员前来处理。

5.1.5 火灾预防和保护

火灾预防：

1) 程远未来运营区域内设置火灾报警装置。在机房内、各物理区域内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位设置烟、温感探测器。
2) 核心区配置独立的气体灭火装置，使用七氟丙烷（HFC-227）等洁净气体灭火系统，备有相应的气体灭火器。程远未来除对纸介质等易燃物质进行灭火外，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂。
3) 火灾自动报警、自动灭火系统避开可能招致电磁干扰的区域或设备，同时配套设置消防控制室。还设有不间断的专用消防电源和直流备用电源，并具有自动和手动两种触发装置。
4) 火灾自动灭火设施的区域内，其隔墙的耐火极限不低于 2 小时，在隔墙上开孔加装甲级防火门。
5) 在管理区和核心区内，设置有紧急出口，紧急出口设有消防门，消防门符合安全要求。紧急出口门与门禁报警设备联动，并装配独立的报警设备。
6) 紧急出口有监控设备进行实时监控，并保证紧急出口门随时可用。程远未来采取适当的管理手段来保障非紧急避险状态下，紧急出口门不能被内部人员任意打开。

灭火系统采用以下方式：

1) 自动控制：将灭火报警联动控制器上控制方式选择键拨到“自动”位置时，灭火系统处于自动控制状态。当保护区发生火情，火灾探测器发出火灾信号，灭火报警联动控制器即发出声、光报警信号，同时发出联动指令，关闭联锁设备，经过一段延时时间，发出灭火指令，打开电磁驱动阀释放启动气体，启动气体通过启动管道打开相应的选择阀和容器阀，释放灭火剂，实施灭火。

2) 电气手动控制：将灭火报警联动器上控制方式选择键拨到“手动”位置时，灭火系统处于手动控制状态。当保护区发生火情，可按下手动控制盒或控制器上启动按钮即可启动灭火系统释放灭火剂，实施灭火。

3) 机械应急操作：当保护区发生火情，控制器不能发出灭火指令时应通知有关人员撤离现场，关闭联动设备，然后拔出相应电磁驱动阀上的保险销，压下手柄即可打开电磁驱动阀，释放启动气体，即可打开选择阀、容器阀、释放灭火剂，实施灭火。如此时遇上电磁驱动阀维修或启动钢瓶充换氮气不能工作时，可打开相应的选择阀手柄，敞开压臂，打开选择阀，然后，用容器阀上的手动手柄打开容器阀，释放灭火剂，实施灭火。

当发出火灾警报，而发现有异常情况，不需启动灭火系统进行灭火时，可按下手动控制盒或控制器上的紧急停止按钮，即可阻止灭火指令的发出。

5.1.6 介质存储

程远未来将储存软件、数据、归档、审计或备份信息的介质保存在安全设施中，这些设施受到适当的物理和逻辑访问控制的保护，只允许授权人员的访问，并防止这些介质受到意外损坏（如水、火灾和电磁等）。

5.1.7 废弃物处理

当程远未来存档的敏感数据或密钥已不再需要或存档的期限已满时，应当将这些数据进行销毁。写在纸张上的，必须切碎，使信息无法恢复。密码设备在作

废处置前根据制造商的指南将其物理销毁或初始化。其他介质以不可恢复原则进行相应的销毁处理。

5.1.8 异地备份

程远未来对关键系统数据、审计日志数据和其他敏感信息进行定期备份，这些备份信息保存在程远未来运营机房以外的其他城市的安全地方。

5.2 程序控制

5.2.1 可信角色

电子认证服务机构、注册机构、依赖方等与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，必须由可信人员担任。程远未来的可信角色包括：

1) 安全策略委员会负责人

负责安全策略委员会的组织和管理工作。

2) 密钥管理员及密钥分管人员

密钥管理员负责管理和操作 CA 证书密钥相关设备；密钥分管人员是分割保管服务器密码机管理员 IC 卡和密钥备份 IC 卡的人员。

3) 安全经理

负责对运营场地安全、人员安全、信息系统安全、通信系统安全、及重要 IT 资产安全进行安全策略的制定和审计的专业人员。

4) 物理场地安全人员

负责运营场地门禁监控、照明、电力、空调、消防、综合布线、静电防护、防雷、防灾等各项基础设施进行日常监控和维护，保障运营场地、机电基础设施正常工作。

5) 运行维护人员

包括网络安全维护、数据库维护、系统维护、CA 系统管理的专业维护人员。网络安全维护人员负责内外网络的安全维护管理，制定网络策略。数据库维护人员负责维护数据库系统。系统管理人员负责对办公系统、电子认证系统进行维护。CA 系统管理人员负责对电子认证服务体系在本单位的系统进行日常管理，执行

系统的日常监控，并可根据需要签发下级操作员证书。

6) 鉴别验证服务人员

负责进行订户证书的信息录入、验证、审核、制证等业务操作，直接对订户提供客户服务。

7) 客户档案管理员

负责客户资料档案的保存和管理。

8) 审计员

负责定期对系统运营状况、业务规范、安全制度执行情况进行检查与审计。

9) 财务经理

负责财务综合管理和风险评估，降低财务风险和机构运营风险。

10) 人事经理

负责人员的背景调查、入职、培训、上岗、转岗、离职等人事工作，负责可信人员管理制度的建立。

5.2.2 每个角色的识别与鉴别

在执行以下操作前，程远未来对服务于关键岗位的人员进行鉴别。

- 为运营区域的所有人员分配用于访问物理场地的权限，并发放访问权限所需的人脸识别、门禁卡、指纹录入、钥匙等；
- 对进入机房区域的人员分配门禁卡并录入指纹；
- 对需要访问电子认证服务系统的人员，为其发放存储介质为 USB KEY 的数字证书。

身份鉴别应包括：由人事职能或安全管理的可信人员对被调查人的身份进行当面的核查，并要求被调查人提供有效身份证件。更进一步的背景调查按照§5.3.2 的要求进行。

5.2.3 需要职责分割的角色

所谓职责分割，是指如果一个人担任了完成某一职能的角色，就不能再担任完成另一特定职能的角色。要求职责分割的角色包括（但不限于）以下几种：物

理场地安全管理员、运行维护人员、密钥管理员、证书鉴别验证人员、客户档案管理员。

5.3 人员控制

5.3.1 资格、经历和无过失要求

所有的员工与程远未来签订保密协议。在程远未来担任一定角色、执行一定功能、完成一定工作的人员，其所受教育、培训及工作经历应足够胜任其工作。程远未来要求充当可信角色的人员至少必须具备诚实、可信赖及工作的热诚度、无影响 CA 运行的其它兼职工作、没有伪造教育工作经历、无同行业重大错误记录、无违法记录等。

5.3.2 背景审查程序

为了确保人员能够胜任有关工作，在成为程远未来的可信人员前，有关人员必须提交相关材料，以证明他们能够胜任预期的工作。

程远未来依据有关材料进行背景调查，在调查过程中，程远未来将为有关人员保密，保护其隐私。背景调查时如果出现提交材料与事实不符或证明提交材料为伪造时，程远未来将拒绝可信职位候选人获得有关职位或取消其可信人员的资格。

5.3.3 培训要求

为了使有关人员能胜任其承担的工作，程远未来对所有入职员工安排专业的培训，培训内容包括：岗位职责、内部规章制度、办公应用软件、操作系统与网络、安全管理要求及制度、事故和安全威胁的报告和处理、业务连续性要求、灾难恢复的办法等。对于从事销售、服务和支持相关岗位的人员，培训还包括：PKI 的相关知识、程远未来的产品与服务、客户服务流程和要求（客服岗位）、认证系统软件安全操作流程等。

程远未来每年会对培训内容进行审查修订。

5.3.4 再培训周期和要求

程远未来对运营相关人员的例行培训每年进行一次，当电子认证服务系统有重大升级改动时或《电子认证业务规则》有重大的内容更新时及时对相关人员进行培训。程远未来的产品与服务培训等根据业务需要安排。

5.3.5 工作轮换周期和顺序

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

5.3.6 对未授权行为的处罚

当程远未来员工被怀疑，或者已进行了未授权的操作，程远未来得知后将立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施，包括警告、罚款甚至辞退。对情节严重的，依法追究其相应责任。

5.3.7 独立合约人的要求

在有限制的情况下，独立合约人或顾问可以担任可信职位。任何合约人或顾问在某一职务的职能和安全标准应与相应职位的内部雇员一样。

担任可信角色的独立合约人和顾问需要通过§5.3.2 中所述的背景调查程序，否则，他们不能担任可信角色；当进入敏感区时，只能在程远未来授权人员的陪同和直接监督下访问认证机构的安全设施，完成有关的工作。

5.3.8 提供给员工的文档

程远未来向员工提供完成其工作所必须的文档，包括但不限于行政、人事、财务、运营管理、机房维护等相关管理制度和规范，员工岗位职责、员工培训资料等，但这些资料通常是不公开的。

5.4 审计日志处理流程

5.4.1 记录事件的类型

程远未来记录与系统相关的事件，这些记录信息称为日志。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) 证书生命周期中的各项操作，包括证书申请、证书更新、证书撤销等事件；
3) 系统、网络安全记录，包括入侵检测和防御系统的记录、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；
4) 系统巡检记录。

对于这些日志，无论其载体是纸张还是电子文档的形式，必须包含事件发生的日期、事件的发生时间段、事件的内容和事件相关的实体等。程远未来还可能记录与系统不直接相关的事件，例如：物理设施的访问记录、可信人员变更记录等。

5.4.2 处理或归档日志的周期

程远未来每天对电子认证服务系统、网络安全设备、操作系统、数据库、动环系统记录等进行处理和分析，每周对上述日志进行审计和备份，每月对上述日志进行归档。

5.4.3 审计日志的保存期限

审计日志被处理后，在程远未来数据中心至少保留 5 年。

5.4.4 审计日志的保护

程远未来执行严格的管理，确保只有程远未来授权的人员才能对审查日志进行相应操作。日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、

修改和删除等。审计日志的制作和访问进行岗位分离。

5.4.5 审计日志备份程序

程远未来保证所有的审查记录和审查总结每周进行备份。

5.4.6 审计日志收集系统

对于电子审计信息，应用程序、网络和操作系统等都会自动生成审计数据和记录信息，自动或人工完成审计信息的收集，电子审计信息刻盘介质由档案管理员进行保管。对于纸质的审计信息，则有专门的文件管理柜来实现审计信息的收集，纸质的审计文件由档案管理员进行保管。

5.4.7 对导致事件实体的通告

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

程远未来定期对电子认证服务系统进行系统风险评估，并形成系统风险评估报告，以降低系统运行的风险。

系统风险评估每年一次。

5.5 记录归档

5.5.1 归档记录的类型

程远未来的归档记录包括所有§5.4 涉及的审计数据、证书申请信息、与证书申请相关的信息等。

5.5.2 归档记录的保存期限

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

1) 对订户证书生命周期内的管理事件的归档，保留 5 年以上。
2) 对 CA 证书和密钥生命周期内的管理事件的归档，在 CA 证书和密钥生命周期之外额外保留 5 年。
3) 订户证书的资料归档保留期限不少于证书失效后 5 年。
4) CA 证书和密钥的归档在 CA 证书和密钥生命周期之外，额外保留 10 年。

5.5.3 归档文件的保护

程远未来的存档内容有物理安全措施的保证，电子存档内容还有密码技术的保护。只有经过授权的工作人员按照特定的安全方式才能查询。程远未来对电子存档数据采用不可擦除光盘保存相关的档案内容，以避免遭受恶劣环境的威胁和破坏，如温度、湿度和强磁力等。

5.5.4 归档文件的备份程序

所有归档文件和数据库备份除了保存在程远未来机房服务器，还在异地保存其备份。数据库备份一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。程远未来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 归档记录的时间标记要求

所有归档记录都要在存档时加具体准确的时间标识以表明存档时间。系统产生的记录，由系统自动添加时间，但这些时间未使用 PKI 时间戳技术。

5.5.6 获得和检验归档信息的程序

程远未来设有专门的档案管理人员统一负责归档信息的存管。

5.5.7 访问和检验归档记录的流程

只有被授权的可信人员才可以查看和获得归档信息，所有归档记录的调用查阅记录需填写记录登记表，调用查阅后重新归档之前进行完整性检验。

5.6 电子认证服务机构密钥更替

程远未来根 CA 密钥的更替，上报给国家密码管理局，并在其监督下重新生成新的密钥和证书。

当 CA 密钥对的累计寿命超过最大生命期，程远未来将启动 CA 密钥更新流程，替换已经过期的 CA 密钥对。CA 密钥变更按如下方式进行：

1) 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”）；
2) 产生新的密钥对，签发新的上级 CA 证书；
3) 在“停止签发日期”之后，对于批准的下级 CA 或最终用户证书请求，将采用新的 CA 密钥签发证书；
4) 上级 CA 继续利用原来的 CA 私钥签发 CRL 直到利用原私钥签发的最后的证书过期为止。

5.7 损害和灾难恢复

5.7.1 事故和损害处理程序

程远未来已制定各种应急处理方案，规定了相应的事故和损害处理程序，这些应急处理方案有：

- 认证系统应急方案；
- 动力系统应急方案；
- 消防应急方案；
- 网络与信息系统应急方案；
- 安全事故应急处理方案等。

出现重大事故立即上报电子认证服务管理部门。

5.7.2 计算资源、软件和/或数据的损坏

程远未来对业务系统及其他重要系统的资源、软件和数据进行了备份，并制定了相应的应急处理流程，当出现计算机资源、软件和/或数据的损坏时在最短的时间内恢复被损害的资源、软件和/或数据。

5.7.3 实体私钥损害处理程序

当订户证书私钥发生泄露时，应按照§4.9 对订户证书进行撤销处理。

当程远未来的根 CA 证书私钥发生泄露时，应立即撤销该证书，并及时通过尽可能的途径通知订户和依赖方。同时立即上报电子认证服务管理部门，说明私钥泄露的时间、原因以及采取的应急措施。

5.7.4 灾难后的业务连续性能力

针对电子认证服务系统的核心业务系统，证书签发系统和证书接口系统采用双机热备方式；对核心数据库，有本地及异地备份机制。程远未来根据业务连续性计划，在灾难发生后的 48 小时内恢复电子认证服务，恢复点目标控制在 30 分钟内，达到 GBT 20988-2007 《信息安全技术 信息技术灾难恢复》中规定的五级要求。

5.8 电子认证服务机构或注册机构的终止

当程远未来或其授权的注册机构需要暂停或终止电子认证服务时，将按照《中华人民共和国电子签名法》及《电子认证服务管理办法》中对电子认证服务提供者暂停或终止服务的规定进行有关工作。

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 密钥对的生成

1) CA 签名密钥的生成

CA 的签名密钥在服务器密码机内部产生，服务器密码机具有国家密码主管部门的相应资质。CA 密钥的生成、保存和密码模块符合国家密码主管部门的要求，并具有国家密码主管部门的相应资质。

2) RA 密钥的生成

RA 的签名私钥在安全控制下产生，RA 证书由程远未来签发。

3) 订户密钥的生成

订户的密钥对可以由订户、程远未来或程远未来委托的机构生成。生成密钥的软硬件系统应能保护私钥不被丢失、泄露、修改或未经授权的访问。订户负有保护其私钥安全的责任和义务，并承担由此带来的法律责任。

订户的加密密钥由密钥管理系统生成，并通过安全的方式传输给订户。密钥管理系统是由国家密码管理批准运营的专业密钥管理系统，负责为电子认证服务订户产生、备份、恢复加密密钥等服务。

由程远未来或其委托的机构为订户生成密钥的传递要符合的§6.1.2 要求。

6.1.2 私钥传送给订户

订户的私钥由订户自己生成时将不会进行传送。

由程远未来或其委托的机构生成时，将使用离线或者在线的安全方式传递。订户委托程远未来或者其注册机构产生私钥时，程远未来或者其注册机构将通过安全途径将证书私钥传送到最终用户手中，并确保在传送过程中私钥不会被非授权的使用、泄露或损坏。

6.1.3 公钥传送给证书签发机构

订户的签名证书公钥以电子的方式提交给程远未来(或通过其授权的注册机构提交)，这些请求通过网络传送时使用安全套接层协议（SSL）和其他安全协议。程远未来接受到订户的证书签名请求文件时，会验证其私钥的数字签名。

6.1.4 电子认证服务机构公钥传送给依赖方

依赖方访问程远未来网站下载 CA 证书，从而得到 CA 的公钥。程远未来的国家根运营 CA 证书还可以通过国家电子认证根 CA 中心网站下载获取。

6.1.5 密钥的长度

程远未来遵从国家法律法规、政府主管机构等对密钥长度的明确规定和要求，目前程远未来支持签发 2048 位 RSA 密钥和 256 位 SM2 密钥的证书。

6.1.6 公钥参数的生成和质量检查

公钥参数由国家密码主管部门许可的加密设备生成，程远未来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。

6.1.7 密钥使用目的

密钥用途应与证书中的“密钥用途”(Key Usage)和“扩展密钥用途”(Extended Key Usage）扩展内容一致。

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

程远未来的根密钥不直接用于签发订户证书。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块标准和控制

程远未来负责生成 CA 证书密钥的密码模块（服务器密码机）放置在程远未来核心区域的屏蔽机房内，使用通过国家密码主管部门鉴定并批准使用的高速服务器密码机设备，其安全性达到以下要求：

1) 接口安全：不执行规定命令以外的任何命令和操作；
2) 协议安全：所有命令的任意组合，不能得到私钥的明文；
3) 密钥安全：密钥的生成和使用必须在硬件密码设备中完成；
4) 物理安全：密码设备具有物理防护措施，任何情况下的拆卸均立即销毁在设备内保存的密钥。

订户可以按照与程远未来签订的相关协议要求选用密码模块，并妥善保管私钥。

6.2.2 私钥多人控制

程远未来 CA 证书私钥存放在服务器密码机中，密钥的生成、更新、撤销、备份和恢复等操作采用多人控制机制，从技术及制度上保证了敏感的加密操作的安全性。服务器密码机的管理员权限采取 5 选 3 的方式，管理员 IC 卡分别由 5 位经过授权的密钥分管员掌握，只有其中 3 名管理员同时在场才能对服务器密码机进行上述操作。

服务器密码机的密钥备份加密导出后，存储介质复制 3 份保存在屏蔽机房的保险箱里。密钥备份文件的加密密钥被分割保存在 5 张备份密钥 IC 卡中，备份密钥 IC 卡分别由 5 位经过授权的密钥分管员掌握，并保存在屏蔽机房的保险箱中。当服务器密码机备份或恢复密钥时，必须由 5 个密钥分管员中的 3 个管理员同时在场才能完成。

订户的私钥由订户自己通过其选用的密码模块控制。

6.2.3 私钥托管

程远未来所有 CA 私钥均未在其他地方托管。程远未来订户密钥的托管参考§4.12 的要求。

6.2.4 私钥备份

CA 私钥由服务器密码机产生，服务器密码机有双机备份，并运行在防高温、防潮、防磁环境中。程远未来对 CA 私钥通过专门的备份卡进行备份，这些备份安全存放于 CA 屏蔽机房的保险柜内。CA 私钥备份和恢复的操作由多人控制，要求参考§6.2.2。

加密私钥由密钥管理中心备份，备份数据以密文形式存在。

6.2.5 私钥归档

当程远未来的 CA 密钥对到期后，这些密钥对将被归档保存至少 10 年（参见§5.5.2）。归档的 CA 密钥对保存在§6.2.1 所述的硬件密码模块中，并且程远未来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，程远未来将按照§6.2.10 所述的方法进行安全地销毁。

订户加密证书密钥对的归档是将已过生命周期或暂不使用的加密密钥以密文形式保存在数据库中，并通过数据库备份出来进行归档保存，归档后的密钥形成历史信息链，供查询和恢复。

6.2.6 私钥导入或导出密码模块

程远未来通过密码模块生成 CA 密钥对，并保存和使用。CA 密钥在与备机传递时，被复制的密钥对以加密的形式在模块之间传送。

通过硬件产生的订户签名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。

6.2.7 私钥在密码模块中的存储

程远未来 CA 证书私钥及其重要组件的私钥在密码模块中加密保存。

6.2.8 激活私钥的方法

程远未来采用硬件设备（服务器密码机）产生、保存 CA 私钥，其私钥激活按照§6.2.2 要求进行管理。

程远未来订户应按照§6.4.1 的要求，在激活私钥之前使用口令或者同等强度的方式进行鉴别，例如：操作私钥需要的口令、操作系统登录口令、屏幕保护口令等。订户应对其工作站进行物理防护，防止未经授权的使用。未激活状态的私钥必须以加密形式保存。

6.2.9 解除私钥激活状态的方法

对于 CA 私钥，当硬件密码模块断电时，私钥进入非激活状态。

订户解除私钥激活状态的方法由其自行决定，例如退出、切断电源、移开令牌或自动锁定等。

6.2.10 销毁密钥的方法

对于程远未来的最终用户证书私钥，若不再使用，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授权使用。若私钥撤销、到期作废后，还需要用于信息解密的，最终用户应该妥善保存一定期限，以便于解开加密信息。若私钥无需再保存，则将通过私钥的删除、系统或密码模块的初始化等安全手段来销毁。

当 CA 的生命周期结束后，程远未来将根据§6.2.5 之相关规定将 CA 私钥进行归档，其它的 CA 私钥备份将被安全销毁。归档的私钥在其归档期结束后，需要在 3 名以上可信人员参与下进行安全地销毁。

6.2.11 密码模块的评估

程远未来使用国家密码主管部门鉴定并批准使用的主机加密设备，符合国家有关标准。密码机采用以分组密码体制为核心的高强度密码算法和非对称密码体

制，密钥采取分层结构，逐层提供保护。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

公钥归档是证书归档的一部分，具体要求参见§5.5。

6.3.2 证书操作期和密钥对使用期限

程远未来 CA 证书和订户证书的操作周期起始于证书被激活，终止于证书过期或者被撤销。程远未来所签发的订户证书的操作周期不能超过 CA 密钥对的使用周期。

公钥和私钥的使用期限与证书的有效期相关但却有所不同。对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期限以外，直到私钥受到损害或密钥对存在被破解的风险，如加密算法被破解。当私钥受到损害或密钥对存在被破解的风险后，签名证书的公钥在技术上仍然可以用于验证数字签名，但这种验证在法律上不一定是有效的。

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

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

另外，无论是订户证书还是 CA 证书的有效期到期后，在保证安全的情况下，允许证书进行更新而不变更密钥对。但是密钥对不能无限期使用，对于不同的证书，密钥对通过证书更新允许的最长使用期限如下：

1) 对于 2048 位 RSA 或 256 位 SM2 根 CA 证书，其密钥对的最长允许使用年限是 30 年；

2) 对于 2048 位 RSA 或 256 位 SM2 其他 CA 证书，其密钥对的最长允许使用年限是 20 年；

3) 对于 2048 位 RSA 或 256 位 SM2 最终用户证书，其密钥对的最长允许使用年限是 5 年。

6.4 激活数据

6.4.1 激活数据的产生和安装

程远未来 CA 私钥激活数据的生成和安装，遵循§6.2.2 对于多人控制的要求。对于订户，激活数据是保护私钥的密码或其他等同安全方式。程远未来推荐订户使用强口令来保证私钥的安全性。

6.4.2 激活数据的保护

程远未来的 CA 密钥管理者（包括密钥分管员）须保护好各自所使用的激活数据 IC 卡。密钥管理者不应对激活数据 IC 卡进行未经授权的使用，也不应向第三方透露任何密钥管理者的身份。

证书订户使用口令或 PIN 码保护私钥，订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。

6.4.3 激活数据的其他方面

存有程远未来 CA 私钥的激活数据 IC 卡，通常保存在程远未来的安全设施中，不能携带外出或传送。如因某种特殊情况确实需要传送时，其传送过程需在程远未来安全管理人员和密钥管理人员的监督下进行。

通常情况下订户证书私钥的激活数据由订户自己产生、保管，不应传送给其他人员，若私钥激活数据因特别的原因需要进行传送时，需要采取加密等保护措施，以防丢失。

当程远未来 CA 私钥激活数据超过§5.5.2 要求的记录保留期限后，程远未来会通过覆盖原有记录或者物理销毁的方式来销毁激活数据。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

程远未来的 CA 系统位于屏蔽机房内，与其他系统隔离。CA/RA 系统的安全防护设置有防火墙、入侵检测与防御系统、漏洞扫描系统。防火墙仅对必要的端口开放访问。

为了保证系统的正常运行，采用的安全技术和控制措施包括：采用安全可信任的操作系统、严格的身份识别和人员访问控制制度、人员职责分割、内部操作控制、业务持续计划等各方面。

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、主要维修过程及与维修有关的情况等；
5) 设备维修时，必须派有专人在场监督。

6.5.2 计算机安全评估

程远未来证书认证系统已通过国家密码管理局等有关部门的安全性审查。

6.6 生命周期技术控制

6.6.1 系统开发控制

程远未来的电子认证服务系统由符合国家相关安全标准和具有商用密码产品生产资质的可靠开发商开发，采用先进的安全控制理念，同时应兼顾开发环境的安全、开发人员的安全、产品维护期的配置管理安全。系统设计和开发运用软件工程的方法，做到系统的模块化和层次化。

6.6.2 安全管理控制

程远未来系统安全管理，严格遵循行业主管部门的规范进行操作，系统的任何变更都经过严格的测试验证后才能进行安装和使用。通过日志检查来检查系统和数据完整性和硬件的正常操作。

程远未来配备了漏洞扫描等专业工具定期对电子认证服务系统进行安全性检查，并对检测结果及时处理，如系统补丁升级、更新安全策略等。系统升级和配置改动都严格遵守《系统变更制度》、《安全管理策略和规范》进行记录和审批。

6.6.3 生命周期的安全控制

整个系统由符合国家相关安全标准和具有商用密码产品生产资质的可靠开发商开发，从设计到实现系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计，使用了基于标准的强化安全通信协议确保了通信数据的安全，在系统安全运行方面，充分考虑了人员权限、系统备份、密钥备份等安全运行措施，整个系统安全可靠。

6.7 网络的安全控制

系统网络安全的主要目标是保障网络基础设施、主机系统、应用系统及数据库运行的安全。程远未来采取防火墙、病毒防治、入侵检测和防御、漏洞扫描、数据备份、灾难恢复等安全防护措施。

6.8 时间标记

程远未来的证书、CRL、OCSP、电子认证服务系统日志均包含时间信息，该时间信息来源于标准时间源。

7 证书、证书撤销列表和在线证书状态协议

7.1 证书

程远未来签发的证书符合 X.509 V3 格式。遵循 RFC 5280 标准。

7.1.1 版本号

版本号为 X.509 V3。

7.1.2 算法对象标识符

符合国家密码主管部门批准的算法对象标识符。

7.1.3 名称形式

数字证书中的主体甄别名（Subject DN）是 X.501 目录唯一名字，各属性的编码一般使用 UTF8String。

证书的主体甄别名根据证书类型和应用需求有所不同，一般格式如下：

C=CN,
O={单位名称},
OU={部门名称},
OU={部门名称},
CN={通用名称}

1) C（Country）为 ISO 3166-1 的国家代码，如 CN 表示中国；
2) O（Organization）应为证书主体所属的单位名称全称，个人证书可以没有此属性；
3) OU（Organization Unit）应为证书主体所属单位部门的名称，个人证书可以没有此属性；
4) CN（Common Name）中的内容分为以下几种：
   a) 个人证书中应为证书主体的姓名；
   b) 机构证书中应为证书主体机构的标准名称或简称；

c) 服务器证书应为证书主体设备的域名或者 IP 地址或者设备编码。

5) 除以上名称属性以外，还可以根据实际的应用需求增加其它 X.501 属性，如 E（Email）在个人邮件证书的 Subject DN 中存在，为证书主体的有效电子邮件地址。

7.1.4 证书扩展项

程远未来证书扩展项除使用 IETF RFC 5280 中定义的证书扩展项，还支持私有扩展项。

程远未来采用的 IETF RFC 5280 中定义的证书扩展项包括但不限于：

1) 颁发机构密钥标识符 Authority Key Identifier
2) 主体密钥标识符 Subject Key Identifier
3) 密钥用法 Key Usage
4) 扩展密钥用途 Extended Key Usage
5) 私有密钥使用期 Private Key Usage Period
6) 主体可选替换名称 Subject Alternative Name
7) 基本限制 Basic Constraints
8) 证书撤销列表分发点 CRL Distribution Points
9) 私有扩展项可支持以下类型：
    a) 个人身份证号码 Identify Card Number
    b) 企业工商注册号 IC Registration Number
    c) 企业组织机构代码 Organization Code
    d) 企业税号 Taxation Number
    e) 统一社会信用代码 Unified Social Credit Identifier

7.2 证书撤销列表

程远未来签发的证书撤销列表符合 X.509V2 格式。遵循 RFC5280 标准。

7.2.1 版本号

版本号为 X.509 V2。

7.2.2 CRL 和 CRL 条目扩展项

CRL 扩展项：颁发机构密钥标识符 Authority Key Identifier。

CRL 条目扩展项：不使用 CRL 条目扩展项

7.3 在线证书状态协议

7.3.1 版本号

使用 OCSP 版本 1（OCSPv1）。

7.3.2 OCSP 扩展项

不使用 OCSP 扩展项。

8 电子认证服务机构审计和其他评估

8.1 评估的频率或情形

程远未来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) 根据业务发展情况，对注册机构进行评估。

程远未来每年接受主管部门的年度检查。注册机构的评估将根据业务发展情况，不定期进行。

程远未来至少每半年进行一次内部审计。

8.2 评估者的资质

合规性审计和评估的机构、人员由电子认证服务的主管部门负责确定。

内部审计人员设有专门的审计岗位，为程远未来的可信人员。

8.3 评估者与被评估者之间的关系

外部评估者与被评估者应无任何业务、财务往来或其它利害关系，足以影响评估的客观性。内部审计人员应满足审计岗位的职责和技能要求。

8.4 评估内容

合规性审计和评估的内容由电子认证服务的主管部门负责确定。

程远未来的内部审计和评估的内容包括：

- 物理场地和设施的管理日志；
- 安全监控记录；
- 密码设备操作使用记录；
- CA 证书及密钥维护记录；
- 认证系统运行日志；
- 运营网络安全监测记录；
- 认证系统操作日志；
- 鉴别验证服务记录。

8.5 对问题与不足采取的措施

对评估中发现的问题，程远未来将根据评估报告的内容准备一份书面解决方案，明确对此采取的行动。程远未来将根据国际惯例和相关法律、法规迅速解决问题。

8.6 评估结果的传达与发布

除非法律明确要求，程远未来一般不公开内部评估结果。对程远未来关联方，程远未来将依据签署的协议来公布内部评估结果。

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

根据市场或管理部门的规定自行决定。

9.1.2 证书查询费用

在证书有效期内，对该证书信息进行查询，程远未来不收取查询费用。

9.1.3 证书撤销或状态信息的查询费用

通过 CRL 查询证书是否撤销，程远未来不收取信息访问费用。通过 OCSP 服务查询证书状态，程远未来是否收费视具体的应用情况而定。

9.1.4 其他服务的费用

程远未来可根据请求者的要求，订制各类通知服务，具体服务费用，在与订制者签订的协议中约定。

9.1.5 退款策略

如果由于程远未来的原因，造成订户合同无法履行、订户证书无法使用，程远未来会将有关费用全额退还给订户。

9.2 财务责任

程远未来有充足的财力保证具有维持运作和履行责任的财务能力。程远未来有能力承担对订户、依赖方等造成的责任风险，并依据本 CPS 规定进行赔偿。

当订户或依赖方在使用证书过程中造成损失时，程远未来有义务提供相应的信息，调查损失原因。如果程远未来不能证明自己无过错，则应对终端实体进行赔偿。

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：

- 程远未来和订户之间的商业协议、往来函件等；
- 证书申请材料；
- 审计记录；
- 电子认证服务机构系统操作相关的访问控制信息；
- 电子认证服务机构根据合理的商业判断应理解为保密数据和信息的内容。

除非法律明文规定，程远未来没有义务公布或透露订户数字证书以外的信息。

9.3.2 不属于保密的信息

程远未来《证书策略》、《电子认证业务规则》不属于保密的信息。

与证书有关的申请流程、申请需要的手续、申请操作指南等信息是公开的。程远未来在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。

订户数字证书的相关信息可以通过程远未来目录服务等方式向外公布。程远未来在其目录服务器中公布证书的撤销信息，供网上查询。

9.3.3 保护保密信息的责任

各方有保护自己、其他人员和单位机密信息的责任，并保证不泄露给第三方。不将机密数据和信息用于协议下活动目的之外的其他用途，包括但不限于将此保密信息的全部或部分进行仿造、反向工程、反汇编、逆向推导；在披露时，如果已明确表示机密数据和信息不得复印、复制或储存于任何数据存储或检索系统，接受方不得复印、复制或储存机密数据和信息。

当程远未来在任何法律、法规或规章的要求下，或在法院的要求下必须提供本《电子认证业务规则》中具有保密性质的信息时，程远未来应按照要求，向执

法部门公布相关的保密信息，程远未来无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

9.4 个人隐私保密

9.4.1 隐私保密方案

除非证书申请人主动提供，程远未来保证不会截取任何证书申请人的资料。程远未来应保护证书申请人所提供的，证明其身份的资料。程远未来承诺不会滥用、未经授权使用或者出售证书申请者姓名等任何证书申请者资料。程远未来采取必要的安全措施防止证书申请人资料被遗失、盗用和篡改。

9.4.2 作为隐私处理的信息

证书申请人提供的不构成数字证书内容的资料被视为隐私信息。

9.4.3 不被视为隐私的信息

证书申请人提供的用来构成数字证书内容的资料不认为是隐私信息。数字证书是公开的，通过程远未来目录服务等方式向外公布。

9.4.4 保护隐私的责任

接收到隐私信息的参与者有责任保护隐私信息不被泄漏、使用或发布给第三方。

9.4.5 使用隐私信息的告知或同意

使用隐私信息，须获得本人同意。

9.4.6 依法律或行政程序的信息披露

依照法律或行政程序进行的信息披露，应当符合下列条件之一：

- 政府法律法规的规定并且经相关部门通过合法程序提出申请；

- 法院以及公共权力部门处理因使用证书产生的纠纷时提出申请；
- 具有合法司法管辖权的仲裁机构的正式申请；
- 证书订户以书面形式进行授权。

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

9.4.7 其他信息披露情形

其他信息的披露遵循国家的相关规定及与订户的相关协议。

9.5 知识产权

程远未来保留其签发的证书和证书撤销信息的所有知识产权。任何人可以免费地复制、分发证书和证书撤销列表，只要他们进行完整复制并且证书和证书撤销列表的使用符合相应的依赖方协议。

除非额外声明，程远未来享有并保留对程远未来提供的全部软件的一切知识产权，包括所有权、名称权和利益分享权等。程远未来有权决定关联机构采用的软件系统，选择采取的形式、方法、时间、过程和模型，以保证系统的兼容和互通。注册机构应征得程远未来的同意使用相关的文件和手册，并有责任和义务提出修改意见。

证书申请者保留证书申请中包含的申请者拥有的商标、服务标志或商业名称以及签发给该证书申请者的证书中可辨识名的所有权利。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

程远未来在提供电子认证服务活动过程中的承诺如下：

1) 程远未来遵守《中华人民共和国电子签名法》及相关法律的规定，接受工业和信息化部的指导，对签发的数字证书承担相应的法律责任。

2) 程远未来保证使用的系统及密码符合国家政策与标准，保证其 CA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定。
3) 除非已通过程远未来证书库发出了程远未来的 CA 私钥被破坏或被盗的通知，程远未来保证其 CA 私钥是安全的。
4) 程远未来签发给订户的证书符合程远未来的 CPS 的所有实质性要求。
5) 程远未来将向证书订户通报任何已知的、将在本质上影响订户的证书的有效性和可靠性事件。
6) 程远未来将及时撤销证书。
7) 程远未来拒绝签发证书后，将立即向证书申请人归还所付的全部费用。
8) 证书公开发布后，程远未来向证书依赖方证明，除未经验证的订户信息外，证书中的其他订户信息都是准确的。

9.6.2 注册机构的陈述与担保

程远未来授权的注册机构在参与电子认证服务过程中的承诺如下：

1) 提供给证书订户的注册过程完全符合程远未来的 CPS 的所有实质性要求。
2) 在程远未来生成证书时，不会因为注册机构的失误而导致证书中的信息与证书申请人的信息不一致。
3) 注册机构将按 CPS 的规定，及时向程远未来提交证书申请、撤销、更新等服务请求。

9.6.3 订户的陈述与担保

订户一旦接受程远未来签发的证书，就被视为向程远未来、注册机构及信赖证书的有关当事人作出以下承诺：

1) 订户需熟悉本《电子认证业务规则》的条款和与其证书相关的证书政策，还需遵守证书持有人证书使用方面的有关限制；
2) 订户在生成数字签名时，证书已经被订户接受且没有过期或撤销。

3) 订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，可供程远未来或其授权的注册机构检查和核实；
4) 订户应当妥善保管和使用私钥，采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件的发生；
5) 一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄密以及其他情况，订户应立刻通知程远未来或注册机构，申请采取撤销等处理措施；
6) 订户已知其证书被冒用、破解或被他人非法使用时，应及时通知程远未来撤销其证书；
7) 按照程远未来 CP 和 CPS 将证书用于规定的使用目的，不将证书用于证书使用目的以外的应用场景。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉本《电子认证业务规则》的条款以及和订户数字证书相关的证书政策，并确保本身的证书用于申请时预定的目的。依赖方在信赖订户的数字证书前，必须采取合理步骤，查证订户数字证书及数字签名的有效性。所有依赖方必须承认，他们对证书的信赖行为就表明他们承认了解本《电子认证业务规则》的有关条款。依赖方对未履行《电子认证业务规则》中规定的依赖方义务而带来的后果承担法律责任。

9.6.5 其他参与者的陈述与担保

其他参与者的陈述与担保同§9.6.4。

9.7 免责声明

为了特定的商业目的，在法律允许的范围内，各参与方可以通过订户协议、依赖方协议或其他订户协议，对自身的某些义务给予免除。

9.8 赔偿责任限制

程远未来不对其签发的证书适用于其规定的目的以外的任何应用承担任何担保，对证书在其规定的目的以外的应用不承担任何责任。对由不可抗力，如战争、地震、洪灾、爆炸、恐怖活动等，造成的服务中断并由此造成的客户损失，程远未来及注册机构不承担责任。

9.8.1 赔偿责任范围

程远未来的赔偿责任范围：

1) 证书信息与订户提交的信息资料不一致，导致订户损失。
2) 因程远未来原因，致使订户无法正常验证证书状态，导致订户利益受损。
3) 程远未来在证书有效期限内承担损失或损害赔偿。

9.8.2 对最终实体的赔偿担保

程远未来对所有当事实体（包括但不限于订户、申请人或信赖方）的合计责任不超过证书的适用的责任封顶。对于一份证书产生的所有数字签名和交易处理，程远未来对于任何人有关该特定证书的合计责任应该限制在一个不超出赔偿责任上限的范围内，这种赔偿上限可以由程远未来根据情况重新制定，程远未来会将重新制定后的情况立刻通知相关当事人。

程远未来所颁发数字证书的赔偿责任上限如下。

1) 个人证书：8000 元人民币；
2) 机构证书：15000 元人民币；
3) 设备证书：20000 元人民币。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的责任均有封顶而不考虑数字签名和交易处理等有关的其他索赔的数量。当超过责任封顶时，可用的责任封顶将首先分配给最早得到索赔解决的一方。程远未来没有责任为每个证书支付高出责任封顶的赔偿，而不管责任封顶的总量在索赔提出者之间如何分配的。

9.8.3 责任免除

有下列情况之一的，应当免除程远未来之责任。

1) 如果证书申请人故意提供了不完整、不可靠或已过期的信息，又根据正常的流程提供了必须的审核文件，得到了程远未来签发的数字证书，由此引起的经济纠纷应由证书申请人全部承担，程远未来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。
2) 程远未来不承担任何其他未经授权的人或组织以程远未来名义编撰、发表或散布的不可信赖的信息所引起的法律责任。
3) 程远未来不承担在法律许可的范围内，根据受害者或法律的要求如实提供网上业务中“不可抵赖”的数字签名依据所引起的法律责任。
4) 程远未来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。
5) 程远未来和注册机构不是证书持有人或依赖方的代理人、受托人、管理人或其他代表。程远未来和证书持有人间的关系以及程远未来和依赖方间的关系并不是代理人和委托者的关系。证书持有人和依赖方都没有权利以合同形式或其他方法让程远未来承担信托责任。
6) 由于客观意外或其他不可抗力事件原因而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。关于不可抗力的描述参见§9.17.5。
7) 因程远未来的设备或网络故障等技术故障而导致数字证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“技术故障”引起原因包括但不限于：（1）不可抗力；（2）关联单位如电力、电信、通讯部门而致；。
8) 程远未来已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

9.9 有限责任

程远未来在对外服务过程中只承担对外声明的、在《电子认证业务规则》中

规定的、对外签署的任何协议中所规定的有限责任。

程远未来根据本《电子认证业务规则》规定赔付标准并进行赔付。

订户和依赖方的赔偿应在订户协议和依赖方协议中规定。

9.10 赔偿

程远未来按照本《电子认证业务规则》§9.8 条款承担赔偿责任。证书订户和依赖方在使用或信赖证书时，若有任何行为或疏漏而导致程远未来和注册机构产生损失，订户和依赖方应承担赔偿责任。订户接受证书就表示同意在以下情况下承担赔偿责任。

1) 未向程远未来提供真实、完整和准确的信息，而导致程远未来或有关各方损失。
2) 未能保护订户的私钥，或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用时。
3) 在知悉证书密钥已经失密或者可能失密时，未及时告知程远未来，并终止使用该证书，而导致程远未来或有关各方损失。
4) 订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个数字签名后理所当然地相信这些表述，订户必须对这种行为的后果负责。
5) 证书的非法使用，即违反程远未来对证书使用的规定，造成了程远未来或有关各方的利益受到损失。

9.11 有效期限与终止

9.11.1 有效期限

除非程远未来特别声明本《电子认证业务规则》提前终止，在程远未来颁布新版本《电子认证业务规则》之前，本《电子认证业务规则》一直有效。

9.11.2 终止

当新版本的《电子认证业务规则》正式发布生效时，旧版本的《电子认证业

务规则》自动终止。

9.11.3 效力的终止与保留

《电子认证业务规则》的某些条款在终止后继续有效，如知识产权承认和保密条款。

9.12 对参与者的个别通告与沟通

认证活动的某一参与方与另一参与方进行通信时必须使用安全通道，以使其通信过程在法律上有效。

9.13 修订

9.13.1 修订程序

当本《电子认证业务规则》不适用时，由程远未来安全策略委员会组织 CPS 编写小组进行修订。CPS 编写小组每年至少审查一次本 CPS，确保其符合国家法律法规和主管部门的要求，修订完成后程远未来安全策略委员会进行审批，审批通过后将在程远未来的网站上发布新的《电子认证业务规则》。《电子认证业务规则》将进行严格的版本控制。

9.13.2 通告机制和期限

本《电子认证业务规则》在程远未来的网站上发布。版本更新时，最新版本的《电子认证业务规则》在程远未来的网站发布，对具体个人不做另行通知。

9.13.3 必须修改业务规则的情形

当管辖法律、适用标准及操作规范等有重大改变时，必须修改《电子认证业务规则》。

9.14 争议处理

程远未来、证书订户、依赖方等实体在电子认证活动中产生争端可按照以下步骤解决：

1) 当事人首先通知程远未来，根据本《电子认证业务规则》中的规定，明确责任方；
2) 由程远未来相关部门负责与当事人协调；
3) 若协调失败，可以通过仲裁或司法途径解决；
4) 任何因与程远未来或授权机构就本《电子认证业务规则》所产生的任何争议而提起诉讼的，受程远未来工商注册所在地的人民法院管辖。

9.15 管辖法律

本《电子认证业务规则》在各方面服从中国法律和法规的管制和解释，包括但不限于《中华人民共和国电子签名法》及《电子认证服务管理办法》等。

9.16 与适用法律的符合性

无论在任何情况下，本《电子认证业务规则》的执行、解释、翻译和有效性均适用中华人民共和国的法律。

9.17 一般条款

9.17.1 完整协议

本《电子认证业务规则》将替代先前的、与主题相关的书面或口头解释。

9.17.2 转让

不作规定。

9.17.3 分割性

当法庭或其他仲裁机构判定协议中的某一条款由于某种原因无效或不具执

行力时，不会出现因为某一条款的无效导致整个协议无效。

9.17.4 强制执行

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

9.17.5 不可抗力

不可抗力是指不能预见、不能避免并不能克服的客观情况。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；也可以是社会现象、社会异常事件或者政府行为，如合同订立后政府颁发新的政策、法律和行政法规，致使合同无法履行，再如战争、罢工、骚乱等社会异常事件。在数字证书认证活动中，程远未来由于不可抗力因素而暂停或终止全部或部分证书服务的，可根据不可抗力的影响而部分或者全部免除违约责任。其他认证各方（如订户）不得提出异议或者申请任何补偿。

9.18 其他条款

无规定。