

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

2026 年 6 月

☐ 内部保密

☒ 公开

程远未来 电子认证业务规则

编号：CYWL-II01-2024

版本号：V1.6

重庆程远未来电子商务服务有限公司

发布日期： 2026 年 6 月 29 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-II01-2024		
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)	程远未来各项制度文档		
保密级别	公开	文档版本号	V1.6
制作人	CPS 编写小组	制作日期	2026.5.07
复审人	安全策略委员会	复审日期	2026.6.16
批准人	安全策略委员会	批准日期	2026.6.26
发布人	安全策略委员会	发布日期	2026.6.29
受控状态	☒ 是 ☐ 否		

【版本变更记录】

生效日期	版本	修改内容	修改人	审核/批准人
2017 年 3 月	V1.0	修订了 CRL 的签发频率内容	黄雪梅	安全策略委员会
2018 年 6 月	V1.1	修订了个人身份的鉴别内容	徐蕤、刘磊、刘玉祥、李海波、魏薇	安全策略委员会
2018 年 10 月	V1.2	修订了证书书更新请求的处理内容	徐蕤、刘磊、刘玉祥、李海波、魏薇	安全策略委员会
2020 年 8 月	V1.3	增加了密钥对的生成及私钥传送给订户的内容	刘玉祥、魏薇	安全策略委员会
2024 年 7 月	V1.4	增加了对证书信息审核验证的规定，增加了赔付监督内容和赔偿监督	李海波、文坤云、魏薇	安全策略委员会

		机制的描述。		
2024 年 11 月	V1.5	增加了预植证书应用说明。	李海波、文坤云、魏薇	安全策略委员会
2026 年 6 月	V1.6	参照《TCQAE 11034-2025 电子认证业务规则规范》修订 CPS	李海波、蔡伟、魏薇、文坤云	安全策略委员会

目 录

1 概括性描述	1
1.1 承诺	1
1.2 基本信息	1
1.3 文档名称与标识	4
1.4 电子认证活动参与者及其职责	4
1.4.1 电子认证服务机构	4
1.4.2 服务机构	4
1.4.3 订户	4
1.4.4 依赖方	5
1.4.5 其他参与者	5
1.5 证书应用	5
1.5.1 证书应用分类	5
1.5.2 证书应用限制	7
1.5.2.1 禁止使用的场景	7
1.6 策略管理	7
1.6.1 策略管理机构	7
1.6.2 策略文档的批准程序	9
1.7 定义和缩写	9
2 信息发布与信息管理	15
2.1 网站发布的内容	15
2.2 信息更新	15
2.3 监管备案	15
2.4 证书信息对接	16
2.5 信息库访问控制	16
3 身份标识与查验	16
3.1 身份查验通用要求	16
3.1.1 通用要求	16
3.1.2 订户告知	16
3.1.2.1 告知内容	16
3.1.2.2 告知方式	17
3.2 初始身份确认	17
3.2.1 证明拥有私钥的方法	17
3.2.2 个人身份的查验	18
3.2.2.1 个人身份信息有效性的确认	18
3.2.2.2 个人高等级证书的实人查验	18

3.2.2.3 个人基础级证书的实人查验	19
3.2.3 机构身份的查验	19
3.2.3.1 机构身份信息有效性的确认	19
3.2.3.2 机构高级等证书的实人查验	20
3.2.3.3 机构基础级证书的实人查验	20
3.3 订户意愿记录	20
3.3.1 订户意愿记录内容	21
3.3.2 个人高等级证书的意愿记录	21
3.3.3 个人基础级证书的意愿记录	21
3.3.4 机构高等级证书的意愿记录	21
3.3.5 机构基础级证书的意愿记录	22
3.4 订户协议	22
3.5 未验证的订户信息	22
3.6 互操作要求	22
3.7 命名	23
3.7.1 命名规则	23
3.7.2 命名有意义，能追溯到唯一实体	23
3.7.3 商标权的处理策略和方式	24
3.7.4 其他自定义内容	24
3.7.5 DN 项结构定义	24
4 证书生存周期操作要求	24
4.1 通用要求	24
4.2 证书申请	25
4.2.1 证书申请实体	25
4.2.2 申请过程与责任	25
4.3 证书签发	26
4.3.1 证书签发过程中电子认证服务机构的行为	26
4.3.2 电子认证服务机构对订户的通告	26
4.3.3 执行识别与鉴别功能	27
4.3.4 证书信息审核验证	27
4.3.5 证书申请批准和拒绝	27
4.4 证书接受	28
4.4.1 向订户交付证书的方式	28
4.4.2 订户接受或拒绝接受证书的步骤和条件	28
4.4.3 订户接受证书的记录和保存	28
4.4.4 电子认证服务机构在颁发证书时对其他实体的通告	29

4.5 密钥对和证书的使用	29
4.5.1 交付前的安全保护	29
4.5.2 私钥管理服务	29
4.5.3 订户私钥和证书的使用	30
4.5.4 依赖方对公钥和证书的使用	30
4.5.5 安全事件反馈	31
4.6 证书续期	31
4.6.1 证书续期的情形	31
4.6.2 请求证书续期的实体	32
4.6.3 证书续期请求的处理	32
4.6.4 颁发新证书时对订户的通告	32
4.6.5 构成接受续期证书的行为	32
4.6.6 电子认证服务机构对续期证书的发布	32
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	32
4.7 证书密钥更新	33
4.7.1 证书密钥更新的情形	33
4.7.2 请求证书密钥更新的实体	33
4.7.3 证书密钥更新请求的处理	33
4.7.4 颁发新证书对订户的通告	33
4.7.5 构成接受密钥更新证书的行为	33
4.7.6 电子认证服务机构对密钥更新证书的发布	33
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	34
4.8 证书变更	34
4.8.1 证书变更的情形	34
4.8.2 请求证书变更的实体	34
4.8.3 证书变更请求的处理	34
4.8.4 颁发新证书时对订户的通告	34
4.8.5 构成接受变更证书的行为	34
4.8.6 电子认证服务机构对变更证书的发布	34
4.8.7 电子认证服务机构对其他实体的通告	35
4.9 证书撤销或冻结	35
4.9.1 证书撤销与冻结的审批流程	35
4.9.2 可请求撤销或冻结的实体	35
4.9.3 请求处理	35
4.9.4 证书撤销的情形	36
4.9.5 撤销请求宽限期	36

4.9.6 电子认证服务机构处理撤销请求的时限	37
4.9.7 依赖方检查证书撤销的要求	37
4.9.8 CRL 的签发频率	37
4.9.9 CRL 发布的最长滞后时间	37
4.9.10 证书状态查询的可用性	37
4.9.11 撤销信息的其他发布形式	38
4.9.12 对密钥遭受安全威胁的特别处理要求	38
4.10 证书状态信息服务	38
4.10.1 证书状态信息服务方式	38
4.10.2 证书状态信息服务响应时间	38
4.10.3 服务可用性	38
4.10.4 备用查询方式	38
4.11 停止使用认证服务	39
4.12 密钥托管与恢复	39
4.12.1 密钥托管与恢复的策略与行为	40
4.12.2 会话密钥的封装与恢复的策略与行为	40
5 认证机构设施、管理和操作控制	40
5.1 物理控制	40
5.1.1 基础设施	40
5.1.2 分区管理和访问控制	41
5.1.3 电力保障	42
5.1.4 门禁与监控	42
5.1.5 灾备	43
5.1.6 环境保障措施	43
5.1.7 消防措施	44
5.1.8 设备管理	45
5.1.9 存储媒体管理	45
5.2 操作过程控制	45
5.2.1 可信角色	45
5.2.2 职责分离	66
5.3 人员控制	66
5.3.1 可信人员资格要求	66
5.3.2 可信人员培训要求	67
5.4 审计日志程序	68
5.4.1 记录范围	68
5.4.2 记录内容	68

5.4.3 保存期限	68
5.4.4 日志审计内容	69
5.4.5 审计周期	69
5.4.6 审计日志备份程序	69
5.4.7 对导致事件实体的通告	69
5.4.8 脆弱性评估	69
5.4.9 审计日志备份程序	70
5.5 记录归档	70
5.5.1 归档范围	70
5.5.2 保存期限	70
5.5.3 保护措施	71
5.5.4 归档记录管理	71
5.5.5 归档记录的类型	71
5.6 电子认证服务机构根证书密钥更替	72
5.6.1 密钥更替程序	72
5.6.2 密钥更替的时间	72
5.7 损害和灾难恢复	73
5.7.1 业务连续性目标	73
5.7.2 恢复流程	73
5.7.3 根私钥应急处理	75
5.7.4 事件报告	75
5.7.5 定期验证	75
5.8 电子认证服务机构终止	75
5.9 重大事项报告	76
6 认证系统技术安全控制	78
6.1 技术安全管理制度要求	78
6.2 密钥对的生成和安装	78
6.2.1 根证书密钥对的生成和安装	78
6.2.2 订户密钥对的生成和交付	79
6.2.3 加密密钥对传递给订户	80
6.2.4 公钥传送给证书签发机构	80
6.2.5 电子认证服务机构公钥传送给依赖方	80
6.2.6 密钥的长度	80
6.2.7 公钥参数的生成和质量检查	81
6.2.8 密钥使用目的	81
6.3 私钥保护和密码模块工程控制	81

6.3.1 CA 私钥保护和密码模块工程控制	81
6.3.2 订户私钥保护和密码模块工程控制	82
6.3.3 私钥托管	83
6.3.4 私钥归档	84
6.3.5 私钥导入或导出密码模块	84
6.3.6 私钥在密码模块中的存储	84
6.3.7 激活私钥的方法	84
6.3.8 解除私钥激活状态的方法	84
6.3.9 销毁密钥的方法	85
6.3.10 密码模块的评估	85
6.4 密钥对管理的其他方面	85
6.4.1 公钥归档	85
6.4.2 证书操作期和密钥对使用期限	85
6.5 激活数据	86
6.6 计算机安全控制	88
6.7 生存周期安全控制	88
6.7.1 系统开发控制	89
6.7.2 安全管理控制	89
6.7.3 生命周期的安全控制	89
6.8 网络的安全控制	89
6.9 时间戳	90
7 证书、证书撤销列表和在线证书状态协议	90
7.1 证书	90
7.2 证书撤销列表	93
7.2.1 版本号	93
7.2.2 CRL 和 CRL 条目扩展项	93
7.3 在线证书状态协议	93
7.3.1 版本号	93
7.3.2 OCSP 扩展项	93
8 认证机构审计及相关评估	94
8.1 审计评估制度	94
8.2 认证业务审计	95
8.3 全面符合性评估	95
8.4 评估结果的传达与发布	96
9 法律责任和其他业务条款	96
9.1 费用	96

9.1.1 证书费用	96
9.1.2 证书查询费用	96
9.1.3 证书撤销或状态信息的查询费用	96
9.1.4 其他服务的费用	97
9.1.5 退款策略	97
9.2 财务责任	97
9.3 业务信息保密	97
9.3.1 保密信息范围	97
9.3.2 非保密信息的范围	98
9.3.3 保护保密信息的信息	98
9.4 个人隐私保护	98
9.4.1 隐私保护方案	98
9.4.2 作为隐私处理的信息	99
9.4.3 不被视为隐私的信息	99
9.4.4 保护隐私的信息	99
9.4.5 使用隐私信息的告知或同意	99
9.4.6 依法律或行政程序的信息披露	99
9.4.7 其他信息披露情形	99
9.5 知识产权	100
9.6 陈述和担保	100
9.6.1 电子认证服务机构的陈述和担保	100
9.6.2 服务机构的陈述和担保	101
9.6.3 订户的陈述和担保	101
9.6.4 依赖方的陈述和担保	102
9.6.5 其他参与者的陈述和担保	102
9.7 担保免责	102
9.8 偿付责任规则	104
9.8.1 偿付责任范围	104
9.8.2 赔付计算方式	104
9.8.3 赔付监督机制	104
9.8.4 责任免除	105
9.9 赔偿	105
9.10 有效期和终止	106
9.10.1 有效期	106
9.10.2 终止	107
9.10.3 效力的终止与保留	107

9.11 对参与者的个别通告与沟通	107
9.12 修订和发布	107
9.12.1 修订程序	107
9.12.2 机制和期限	107
9.12.3 必须修改业务规则的情形	107
9.13 争议处理与举证	108
9.13.1 争议处理	108
9.13.2 举证	108
9.14 管辖法律	109
9.15 与适用法律的符合性	109
9.16 一般条款	109
9.16.1 完整协议	109
9.16.2 分割性	109
9.16.3 强制执行	110
9.16.4 不可抗力	110
9.17 其他条款	110

1 概括性描述

1.1 承诺

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》或 CPS）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》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。

程远未来开展经营和服务活动时，遵守法律、行政法规，树立以人民为中心的服务理念，承担社会责任。与客户建立业务关系前，开展应用业务调研，建立应用接入业务风险评估及内部定责机制，严禁为存在违法违规风险的业务提供电子认证服务；承诺使用经过国家密码管理局审查的电子认证服务系统开展电子认证服务；接受政府和社会监督，对主管部门检查发现的问题及时整改，建立问题纠治长效机制，持续符合整改要求。

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、服务机构、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 基本信息

机构名称：重庆程远未来电子商务服务有限公司；

法定代表人：谷旭阳；

机构住所、经营场所的地址：重庆市两江新区人和街道镜泊中路 5 号远大印务 1 栋 1 层（401121）；

网站地址：<http://www.ifutureca.com>；

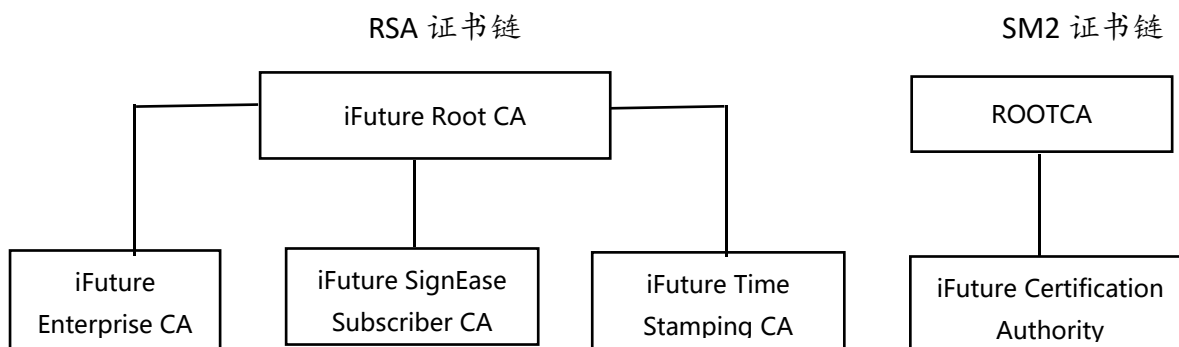
电话号码：023-63063149；

邮箱地址：2243735274@qq.com；

已取得《电子认证服务许可证》，编号为：ECP50011223047，发证机关为：中华人民共和国工业和信息化部，批准日期是 2018 年 11 月 14 日，有效期从 2023 年 11 月 14 日至 2028 年 11 月 13 日；

已取得《电子认证服务使用密码许可证》，证书编号：0047，发证机关：国家密码管理局，批准日期是 2016 年 10 月 26 日，有效期从 2021 年 10 月 26 日至 2026 年 10 月 26 日；

程远未来提供 RSA 签名算法和 SM2 签名算法的证书链（简称 RSA 证书链和 SM2 证书链）。程远未来提供的证书链均为两级。RSA 证书链有 3 个，SM2 证书链 1 个。



RSA 证书链的根证书为程远未来自签根证书,使用的签名算法为 RSA,密钥长度为 2048-bit,有效期为 15 年。基本信息如下:

证书序列号: 070000201906110100162965499829;

颁发机构名称: iFuture Root CA

使用机构名称: iFuture Root CA

计划服务时间至 2033年12月24日 0:00:00。

该根证书下设三个证书，其中 iFuture Time Stamping 证书用于为机构订户签发基于 RSA 算法的时间戳证书,其它两个用于为订户签发基于 RSA 算法的个人证书、机构证书、设备证书:

颁发机构名称	使用机构名称	证书序列号	密码算法	密钥长度	有效期	计划服务时间
iFuture Root CA	iFuture Enterprise CA	070000201906110100864114221521	RSA	2048bit	15年	2033年12月24日 0:00:00
iFuture Root CA	iFuture SignEase Subscriber CA	070000201906110100517621217451	RSA	2048bit	15年	2033年12月24日 0:00:00
iFuture Root CA	iFuture Time Stamping CA	070000201906110100642359618427	RSA	2048bit	10年	2028年12月24日 0:00:00

SM2 证书链的根证书是国家密码管理局的根证书，密码算法为 SM2，密钥长度为 256-bit，有效期 30 年。其它基本信息为：

证书序列号: 69E2FEC0170AC67B

颁发机构名称: ROOTCA

使用机构名称: ROOTCA

计划服务时间至 2042年7月7日 11:11:59。

下设 iFuture Certification Authority 证书,该证书是国家密码局签发的,用于程远未来向订户签发基于 SM2 算法的个人证书、机构证书、设备证书。该证书签名算法：SM2，密钥长度：256-bit。证书序列号为 78AAFFDC5A9D69FACFA4E96A22D19349，颁发机构:ROOTCA，使用机构：iFuture Certification Authority，有效期限：20 年，计划服务时间为至 2038年5月31日 11:16:33 止。

1.3 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》，版本号是 V1.6，遵循的证书策略 OID 是 1.2.156.115251.1.2.1。

1.4 电子认证活动参与者及其职责

电子认证活动参与者包括但不限于 CA、服务机构、订户、依赖方等。

1.4.1 电子认证服务机构

电子认证服务机构是受用户信任，负责鉴证审核、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。

1.4.2 服务机构

服务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：协助收集证书申请人申请资料和信息，并传递给电子认证服务机构。

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服务机构的角色。在不违反本 CPS 及与程远未来签署的协议的前提下，服务机构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和鉴证审核。

1.4.3 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签订合同获得证书，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。

1.4.4 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。

1.4.5 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。

1.5 证书应用

1.5.1 证书应用分类

程远未来签发的电子签名认证证书分为个人签名证书（个人证书）和机构签名证书（机构证书）等。按证书主体对象的类型和风险等级主要分为个人高等级电子签名认证证书、个人基础级电子签名认证证书、机构高等级电子签名认证证书、机构基础级电子签名认证证书等类型。

1.5.1.1 证书分类

1) 个人证书

分为个人高等级电子签名认证证书、个人基础级电子签名认证证书，用于个人身份认证、个人邮件认证等，和需要区分、标识、鉴别个人身份的认证应用，还用于数据加解密和信息签名，包括订单、合同签名，以实现信息加密，提供信息源发性证明、完整性保障和抗抵赖。场景包括：业务系统登

录时的身份唯一性确认、关键或核心数据电子签名验证（含对电子合同、格式文件等进行电子签章）等。

2) 机构证书

分为机构高等级电子签名认证证书和机构基础级电子签名认证证书两类，包括机构部门证书、机构职员证书和机构职位证书（如法人证书等），用于需要区分、标识、鉴别机构身份的应用，还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。适用场景包括：业务系统登录时的身份唯一性确认、关键或核心数据电子签名验证（含对电子合同、格式文件等进行电子签章）等。

1.5.1.2 证书分级及使用场景

1) 基础级电子签名认证证书

适用于除 § 1.5.2 要求之外的低风险业务，如电子政务等高安全系统登录时的身份唯一性确认和关键数据的电子签名（涉及生命健康、财产权益等高风险活动禁止使用基础级电子签名认证证书。）；

2) 高等级电子签名认证证书

在基础级电子签名认证证书适用的业务上，适用于涉及生命健康、财产权益等的高风险业务（不得包括 § 1.5.2.1 的限制）。

表 1 电子签名认证证书分类表

证书类型	主管部门 证书策略 OID	其他 证书策略 OID	含义
个人高等级电子签名 认证证书	2.16.156.339.2.1.1.2	1.2.156.115251.2.1.2	适用于高风险业务、符合《电子签名法》的个人电子签名认证证书
个人基础级电子签名 认证证书	2.16.156.339.2.1.1.1	1.2.156.115251.2.1.1	适用于低风险业务、符合《电子签名法》的个人电子签名认证证书
机构高等级电子签名 认证证书	2.16.156.339.2.1.2.2	1.2.156.115251.2.2.2	适用于高风险业务、符合《电子签名法》的机构电子签名认证证书
机构基础级电子签名 认证证书	2.16.156.339.2.1.2.1	1.2.156.115251.2.2.1	适用于低风险业务、符合《电子签名法》的机构电子签名认证证书

1.5.1.3 其它说明

程远未来签发的数字证书一般为签名证书。如果订户申请签名证书的同时也

申请了加密证书的,该加密证书只能用于数据加解密,不得用于电子签名及验证。

程远未来可为机构订户签发设备证书和时间戳证书。这两类证书仅限于证明设备身份或基于时间戳服务器提供的时间证明等,不适用于电子签名。

程远未来签发的证书中,订户名称是以“测试-”开头或以“-Test”结尾的,均表示为用于测试目的,不适用于电子签名。

程远未来签发的数字证书不具有特殊用途或适用特定行业规范。

1.5.2 证书应用限制

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,如果依赖方或订户不遵守相关约定,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。

涉及生命健康、财产权益等高风险活动禁止使用基础级电子签名认证证书。

1.5.2.1 禁止使用的场景

禁止使用的场景包括但不限于:

- 1) 涉及人身关系的,如婚姻、收养、继承等;
- 2) 涉及停止公共事业服务的,如停止供水、供热、供气等;
- 3) 法律、行政法规规定的其他不适用电子签名的应用场景或类型;
- 4) 国家法律法规禁止的活动;
- 5) 未成年人或限制民事行为能力人。

1.6 策略管理

1.6.1 策略管理机构

程远未来设立了安全策略委员会,并任命安全策略委员会负责人及委员会组成的各个成员。成员名单以及各成员的工作职责公示于公司网站或 CPS。每年会不定期进行会议讨论本机构的发展运营战略方针,并妥善保存安全策略委员会重大决议的相关文件和会议记录。

安全策略委员会负责 CPS 和 CP 以及配套制度的维护，包括但不限于以下职责：

a) 确定维护 CPS 和 CP 等策略文档的职能分工，建立合理有效的修订和批准流程；

b) 对涉及信息安全策略、根证书密钥、证书签发自动审核等重要操作和流程进行审批；

c) 每年至少进行一次 CPS 和 CP 全面评审，根据实际需要及时修订策略文档；

d) 每年组织运营风险评估并形成报告。

表 2 程远未来安全策略委员会成员名单

序号	姓名	职位	工作职责
1	李海波	委员会负责人	组建公司安全策略管理组织，并领导该组织工作； 负责定期组织制定和维护公司 CPS，并监督执行； 有效控制公司运营风险，保证电子认证服务质量和业务连续性。
2	卢毅	委员会成员	评估和审核系统策略、系统或应用开发需求、系统架构和安全手段的技术可行性，确保其与公司电子认证业务规则兼容。
3	蔡伟	委员会成员	对信息安全策略、根证书密钥更新等进行审批，确保电子认证业务可顺利执行。
4	魏薇	委员会成员	负责策略的对外发布、咨询及档案管理等日常工作
5	文坤云	委员会成员	接受委员会安排的工作，参与委员会的各项决策讨论和实施。

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。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。

1.6.2 策略文档的批准程序

1) 起草小组的成立流程

由程远未来安全策略委员会组织审批成立 CPS 编写小组。

2) 安全策略委员会的审批流程

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。

3) 向主管机关的备案流程

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。

4) 发布流程

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。

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>

1.7 定义和缩写

1.7.1 定义

下列定义适用于本《电子认证业务规则》:

- 加密 encipherment encryption

对数据进行密码变换以产生密文的过程。

[来源: GB/T 25069—2022,3.278]

- 密码模块 cryptographic module

实现密码运算功能,相对独立的软件、硬件、固件或这三者组合。

[来源: GB/T 25069—2022,3.379]

- 密码算法 cryptographic algorithm

描述密码处理过程的算法。

[来源: GB/T 25069—2022,3.380]

- 密钥 key

控制密码变换操作的符号序列。

[来源：GB/T 25069—2022,3.389]

注：在非对称密码算法中，密钥包括私钥和公钥。

- 私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

[来源：GB/T 25069—2022,3.580]

注：属于《中华人民共和国电子签名法》中电子签名制作数据的一种实现形式。

- 公钥 public key

非对称密码算法中可公开的密钥。

[来源：GB/T 25069—2022,3.211]

注：属于《中华人民共和国电子签名法》中电子签名验证数据的一种实现形式。

- RSA 算法 RSA algorithm

一种基于大整数因子分解问题的公钥密码算法。

[来源：GB/T 25069—2022,3.582]

- SM2 算法 SM2 algorithm

由 GB/T 32918 定义的一种椭圆曲线公钥密码算法。

[来源：GB/T 25069—2022,3.583]

- SM3 算法 SM3 algorithm

由 GB/T 32905 定义的一种密码杂凑算法。

[来源：GB/T 25069—2022,3.584]

- 公钥基础设施 public key infrastructure(PKI)

基于公钥密码技术，具有普适性，可用于提供机密性、完整性、真实性及抗抵赖性等安全服务的基础设施。

[来源：GB/T 25069—2022,3.212]

- 数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性

和签名行为的抗抵赖性。

[来源：GMZ 4001—2013,2.113]

- 电子认证服务机构 certification service provider

取得电子认证服务许可证，为需要第三方认证的电子签名，签发电子签名认证证书并为有关各方提供真实性、可靠性验证的实体。

- 数字证书 digital certificate

也称公钥证书，由认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

[来源：GM/Z 4001—2013,2.115,有修改，删除了分类]

- 电子签名认证证书 electronic signature certificate

由依据《中华人民共和国电子签名法》设立的电子认证服务机构签发的，可证实电子签名人与电子签名制作数据有联系的数字证书。

注 1:如无具体限定，本规范中的“证书”均指“电子签名认证证书”，本规范中的“密钥”“私钥”，均指电子签名认证证书所对应的“密钥”“私钥”。

注 2:可证实电子认证服务机构与电子签名制作数据有联系的数字证书，称为根证书。

- 电子签名依赖方 electronic signature relying party

是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。

注：本文件中简称依赖方。

- 订户 subscriber

被颁发给一张证书的证书主体。[来源：GB/T 26855—2011,3.15]

注：在不同的阶段，也称为证书申请人，证书持有人，属于《中华人民共和国电子签名法》中电子签名人的一种类型。

- 对象标识符 object identifier(OID)

用于无歧义地标识对象的全局唯一值。

[来源：GB/T 25069—2022,3.138]

- 证书策略 certificate policy(CP)

指明证书对于具有普通安全需求的特定团体和/或应用类的适用性的规则集合。

[来源：GB/T 25069—2022,3.780]

- 证书策略对象标识符 CPOID

对某个证书策略进行唯一标识的 OID.

- 证书链 certificate chain

证书链是一个用于证书验证的证书序列

- 身份查验 entity authentication

证实某个实体就是所声称身份的过程。

- 激活数据 activation data

用于使密码模块进入可操作状态的数据。可为口令、生物特征等。

[来源：GB/T 25069—2022,3.267]

- 时间戳 time stamp(TS)

对时间和其他待签名数据进行签名得到的，用于表明数据时间属性的数据。

[来源：GB/T 25069—2022,3.541]

- 证书续期 certificate renewal

指在不改变订户信息的情况下，用一个新证书来代替旧证书的过程。

- 密钥更新 key re-key

用新密钥替换旧密钥的过程。

[来源：GB/T 25069—2022,3.400]

注：通常指证书与密钥同时更新。

- 密钥恢复 key recovery

将归档或备份的密钥恢复到可用状态的过程。

[来源：GB/T 25069—2022,3.405]

- 证书撤销列表 certificate revocation list(CRL)

由电子认证服务机构签发并发布的被撤销证书的列表。

[来源：GB/T25069—2022,3.781,有修改，证书认证机构改为电子认证服务机构]

- 高等级电子签名认证证书 enhanced electronic signature certificate

适用于涉及生命健康、财产权益等高风险场景的电子签名认证证书。

- 基础级电子签名认证证书 qualified electronic signature certificate

适用于除高等级证书规定场景外的其他电子签名场景的证书。

- 证书认证系统 CA system

对数字证书的申请、签发、发布、更新、撤销、验证等数字证书全生存周期进行管理和服务的系统。

[来源：GB/T 25069—2022,3.787,有修改，扩充了申请、验证和服务等内容]

注：也称电子认证服务系统，包括证书签发子系统、证书注册子系统等。

- 注册机构（RA）Registration Authority

注：本文件中也称为认证机构，简称 CA.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。

- 证书主体 Subject

证书主体是证书中的“主体”（Subject）项指定的、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。

- 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。

- 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。

- 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。

- 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。

- 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。

- 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。

- 协同签名 collaborate signature mechanism

签名方与程远未来各自保存部分密钥分量,通过相互协同配合完成电子签名的机制。

- 代理签名 delegated signature mechanism

签名方将密钥托管在程远未来,并授权程远未来完成电子签名的机制。

1.7.2 缩写

下列缩略语适用于本文件。

CA:电子认证服务机构(Certification Authority)

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

CP:证书策略(Certification Policy)

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

DN:甄别名称(Distinguished Name)

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

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

OID:对象标识符(Object Identifier)

RTO:恢复时间目标(Recovery Time Objective)

RPO:恢复点目标(Recovery Point Objective)

2 信息发布与信息管理的

2.1 网站发布的内容

程远未来公司网站发布的内容，包括但不限于：

- 1) 程远未来证书策略和电子认证业务规则的所有版本；
- 2) 证书链；
- 3) 证书信息、状态信息等查询服务；
- 4) 详细的业务办理指南，包括但不限于服务网点地址、营业时间、联系电话等；
- 5) 依赖方协议；
- 6) 投诉处理政策及投诉方式，包括但不限于：投诉处理部门的地址、联系电话、电子邮件地址，以及内部监督部门名称。

2.2 信息更新

网站信息发布内容如有变化，本机构将在生效后 1 个工作日内更新。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 监管备案

按照国家电子认证服务管理平台的要求进行相关备案。

2.4 证书信息对接

按国家和监管部门的要求完成与国家电子认证服务管理平台的技术对接，实现根据证书唯一编码、订户身份信息等维度查询本机构已签发证书列表的功能。

2.5 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。

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。

§ 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 身份标识与查验

3.1 身份查验通用要求

3.1.1 通用要求

在进行受理证书申请时，程远未来会对订户和/或受托人进行告知、身份确认、意愿记录和协议签署；

对于订户的身份查验义务,程远未来不会委托给外部机构或个人（非属同一法人主体的机构视为外部机构）。

3.1.2 订户告知

3.1.2.1 告知内容

订户申请证书时，程远未来将告知订户相关情况，包含订户的权利和义务，

服务收费的项目和标准，电子签名认证证书、电子签名的使用条件，信息安全保障措施，程远未来和订户的责任划分，订户签名私钥的存储方式、安全要求以及订户不得将所获证书用于任何违法违规或违背公序良俗的用途，不得利用证书从事侵害国家利益、社会公共利益以及第三方合法权益的活动。

3.1.2.2 告知方式

1) 程远未来签发高等级证书时，采用面对面、电话、视频或主管部门认可的其他方式告知，并保留告知的记录；

2) 程远未来签发基础级证书时，采用与高等级证书相同的告知方式，或采用强制阅读、短信、邮件等方式告知，并保留告知的记录。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

1) 按照 § 6.2.2 规定的方式生成订户密钥对；

2) 通过数字签名的方式来确认证书订户拥有某个公钥对应的签名私钥。

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，程远未来用其对应的公钥来验证这个签名。如果密钥对是程远未来为订户生成的，则不需要进行上述证明，但加密密钥对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(含与密钥匹配的 PIN 码/验证密码)，证书申请人被视作其私钥的唯一持有者。

3.2.2 个人身份的查验

3.2.2.1 个人身份信息有效性的确认

个人订户申请证书时，应向程远未来提供真实有效的个人身份信息。程远未来先对申请材料进行初步完整性检查，再对证书申请者的身份信息进行查验。对个人身份信息的查验方式和内容如下：

- 1) 受理个人证书申请时，程远未来将要求订户出示其有效身份证件或有效身份证件信息（有效证件类型仅限法律法规和国家有关文件规定的身份证件的原件或扫描件，例如：身份证、护照、港澳居民来往内地通行证、台湾居民来往大陆通行证、外国人永久居留证等）；
- 2) 通过证件机读工具、权威数据库或主管部门认可的其他方式查验订户身份证件的真实性和有效性；程远未来采用包括但不限于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，例如：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。
- 3) 当订户委托他人代为办理时，除查验订户本人签署的有效书面授权证明外，受托人本人还应向程远未来出示其有效身份证件或有效身份证件信息，并按照 2) 款方式查验订户和受托人的身份证件或身份资料。

3.2.2.2 个人高等级证书的实人查验

程远未来对订户开展实人查验采用下列方式之一：

- 1) 面对面查验；
- 2) 远程人工面对面查验；
- 3) 生物特征验证：如活体人脸、指纹、声纹、掌纹等生物识别技术的应用；
- 4) 通过主管部门认可的其他方式；

程远未来以可追溯的方式完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

3.2.2.3 个人基础级证书的实人查验

程远未来对订户开展实人查验采用下列方式之一：

- 1) 通过第 § 3.2.2.2 规定的方式；
- 2) 电信运营商三要素：核对姓名、证件号码、手机号码在电信运营商系统中的一致性，并通过对应手机号的随机短信验证码核验；
- 3) 银行卡四要素：核对姓名、证件号码、银行卡号、银行预留手机号在银行系统中的一致性，并通过预留手机号的随机短信验证码核验；
- 4) 由申请人持有的有效电子签名认证证书签名验证；
- 5) 通过主管部门认可的其他方式，如居民身份网络可信凭证、公民网络电子身份标识、国家网络身份认证系统、内地银行或支付机构对外提供的个人账户和身份信息对应关系验证等。

程远未来以可追溯的方式完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

3.2.3 机构身份的查验

3.2.3.1 机构身份信息有效性的确认

签发机构证书、设备证书时，需确认组织机构是真实存在的、合法的实体。机构订户需要向程远未来提交政府签发的组织机构成立的有效文件，并确认该组织机构知晓并同意受托人的授权申请，程远未来对组织机构进行身份信息查验，方式及内容如下：

- 1) 机构有效证件的查验方式：程远未来通过权威的第三方数据库确认其有效证件的真实性（有效证件类型仅限法律法规和国家有关文件规定的证件，例如：营业执照、组织机构代码证、事业单位法人证书、民办非企业单位登记证书、医疗机构执业许可证、律师事务所执业许可证等原件或扫描件）；
- 2) 法定代表人或受托人的身份查验方式：
 - a) 法定代表人或受托人身份证件信息查验方式参见 § 3.2.2.1；
 - b) 受托人办理时，应提供组织机构加盖公章的有效书面授权证明，以证明其提

交证书申请的行为已获得授权。程远未来应查验该书面授权证明。

3.2.3.2 机构高等级证书的实人查验

对订户开展实人查验采用下列方式之一：

- a) 法定代表人实人查验，方法见 § 3.2.2.2；
- b) 受托人实人查验，方法见 § 3.2.2.2，并通过机构对公账户随机金额打款验证或主管部门认可的其他方式。

程远未来受理机构证书业务中的机构部门证书、机构职员证书和机构职位证书（如法人证书等），按机构证书进行查验。受理该组织机构的设备证书时，程远未来除了对组织机构进行身份查验，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。确认的方式可以通过域名注册商确认域名所有者信息。

程远未来以可追溯的方式完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

3.2.3.3 机构基础级证书的实人查验

程远未来对订户开展实人查验采用下列方式之一：

- 1) 法定代表人实人查验，方法见 § 3.2.2.3；
- 2) 受托人实人查验，方法见 § 3.2.2.3；
- 3) 由订户持有的同等级或更高级的有效机构证书签名验证；

程远未来会完整记录并保存身份查验过程和结果。每张证书建立独立的身份验证记录。

3.3 订户意愿记录

订户向程远未来申请数字证书时，程远未来将通过多种方式，例如页面显示、音频视频朗读等向订户展现意愿记录的方式，并经订户点击/手写签字/视频点头确认等方式，确认订户知晓且同意本次申请的全过程及需要承担的责任和义务。作为订户申请证书材料的一部分，程远未来会以包括录音录像方式在内的多种手

段保留完整、可追溯的订户意愿记录。

3.3.1 订户意愿记录内容

订户意愿记录内容，包括但不限于：

- 1) 订户身份信息；
- 2) 程远未来的信息；
- 3) 签名私钥保存方法及其保存义务；
- 4) 订户对电子签名的法律责任；
- 5) 订户对上述第 1 至第 4 项内容已充分知晓并同意的明确意愿表示。

3.3.2 个人高等级证书的意愿记录

程远未来对订户申请证书时的意愿的确认将采用下列方式之一：

- 1) 现场办理时，通过面对面确认或手抄提示语的方式，并采用录音录像或通过主管部门认可的其他方式记录订户意愿；
- 2) 远程办理时，通过音视频或通过主管部门认可的其他方式确认并记录订户意愿。

3.3.3 个人基础级证书的意愿记录

程远未来对订户申请证书时的意愿的确认将采用下列方式之一：

- 1) 与高等级证书相同的方式，见 § 3.3.2；
- 2) 采用强制阅读、短信或邮件确认等电子方式；

程远未来保留完整、可追溯的订户意愿记录。

3.3.4 机构高等级证书的意愿记录

订户意愿的确认采用下列方式之一：

- 1) 法定代表人申请时，按照 § 3.3.2 的方式确认机构法定代表人的意愿；
- 2) 受托人申请时，查验加盖机构公章的授权文件，并按照 § 3.3.2 的方式确认受托人的意愿。

程远未来将采用录音录像或通过主管部门认可的其他方式记录订户意愿。

3.3.5 机构基础级证书的意愿记录

订户意愿的确认采用下列方式之一：

- 1) 法定代表人申请时，按照 § 3.3.3 的方式确认机构法定代表人的意愿。
- 2) 受托人申请时，查验加盖机构公章的授权文件，并按照 § 3.3.3 的方式确认受托人的意愿。

程远未来会保留完整、可追溯的订户意愿记录。

3.4 订户协议

程远未来的订户协议内容包含 § 3.1.2.1 中规定的所有内容，并且发布于程远未来官网上，供订户及依赖方了解和使用。

3.5 未验证的订户信息

- 1) 证书载明信息的查验方法、查验流程按照 § 3.2.2 和 § 3.2.3 执行。
- 2) 证书中不包含未经验证的订户信息。

3.6 互操作要求

互操作业务情形中 CA 的义务和责任。

互操作业务情形可能是交叉认证、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。

互操作业务中均由 CA 证书颁发机构方承担鉴证、校验、验签等职责，CA 的义务和责任并不由互操作改变。

3.7 命名

3.7.1 命名规则

依 X.501 甄别名命名规则解释。根据个人和机构等不同类型的证书，分别约定了其命名规则：

个人命名规则主体 DN 项中包含订户姓名，在 DN 项或扩展项中包含有效证件类型及其编号（或相关信息的映射，包括但不限于散列值、掩码等）。

机构命名规则是主体 DN 项中包含机构名称，在 DN 项或扩展项中包含组织机构的有效证件类型及其编号。

3.7.2 命名有意义，能追溯到唯一实体

订户证书的主体甄别名（DN）必须具有一定的代表意义。

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（同一订户需要申请多张证书时，在其 DN 项中添加申请的顺序号，以表示该订户申请的第几张证书。添加的顺序号（包括顺序号的前后缀符号等）不属于订户名称的一部分），其中的例外是签发双证书时（即同时签发签名证书和加密证书），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。

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或脱敏的。

机构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。

3.7.3 商标权的处理策略和方式

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。

3.7.4 其他自定义内容

在不影响证书通用性的前提下,可在证书中增加自定义的其他内容。

3.7.5 DN 项结构定义

DN 项结构定义符合 GB/T16264.8 的要求,证书主体 DN 项编码规则见下图;

代码	说明	示例
C	国家	CN
S	省份(可选)	北京
L	城市(可选)	北京
O	订户所在机构信息	**公司
OU	订户所在机构部门信息	**部门
CN	订户名称(个人姓名或机构法定名称)	张三/**公司或张三(1)/**公司(1)

4 证书生存周期操作要求

4.1 通用要求

该 CPS 中各方的责任包括但不限于:

- 1) CA 承担建立、运营和维护注册通道的责任;
- 2) CA 承担与订户签订电子认证服务协议的责任;
- 3) 订户承担提供准确信息的责任;
- 4) CA 承担妥善记录并保存相关信息的责任。

4.2 证书申请

证书申请处理的流程：按照 § 3 规定，完成对订户的告知、身份确认、意愿记录、协议签署等步骤，并依据既定准则批准或拒绝该申请；

证书申请处理的时限：程远未来应做出合理努力来尽快确认证书申请信息，自受理之日起完成证书申请处理的最长期限为不超过两个工作日，因特殊情况确需超期的，应与订户协商确定处理时限。

4.2.1 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托人申请。
- 组织机构申请机构证书时，由法定代表人或机构授权人员申请。
- 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。

4.2.2 申请过程与责任

证书申请者可在线申请或到程远未来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。

4.3 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，程远未来有义务在证书申请处理完毕后向订户通告处理结果，通告结果的方式包括但不限于：

- 1) 通过认证应用工具进行信息提示；
- 2) 通过信函、站内信或电子邮件发送；
- 3) 通过短信通知；
- 4) 通过电话通知；

- 5) 当面通知或通过实时视频等相当于面对面的方式通知;
- 6) 通过主管部门认可的其他方式;

4.3.3 执行识别与鉴别功能

程远未来按照本《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 个人身份的鉴别、§ 3.2.3 机构身份的鉴别。

4.3.4 证书信息审核验证

处理证书申请时,需根据 § 3.2.2 个人身份的鉴别和 § 3.2.3 机构身份的鉴别规则进行鉴别,对证书信息内容进行审核验证。

4.3.5 证书申请批准和拒绝

程远未来根据本《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,程远未来将拒绝证书申请。

- 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)。

4.4 证书接受

4.4.1 向订户交付证书的方式

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。

当与证书订户间有特别的约定时，程远未来可根据订户密钥保存方式，通过人工或自动方式，如（面对面、邮政快递、订户远程下载、私钥管理服务自动下载）等方式向订户交付数字证书。

4.4.2 订户接受或拒绝接受证书的步骤和条件

订户通过面对面的方式从程远未来接受载有证书和私钥的介质的行为，即表明用户接受了证书，不接受证书和私钥的介质时，视为拒绝；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间内未对证书或证书内容提出异议，即表明订户接受了证书。不接收包含证书和私钥的介质的快递，快递包裹持续在快递公司人员手中或发送邮件内容明确不接受证书和私钥的介质，视为拒绝。

订户通过特定站点自行将证书下载到本地数字证书存放介质时，系统记录订户下载了证书即表明订户接受了证书。订户未在两个工作日内下载证书，视为拒绝。

当双方约定证书由程远未来生成并保存时，订户自收到程远未来通知后两个工作日内未明确表示不接受证书或该证书对应的签名私钥已用于产生电子签名，视为订户接受了证书，订户在两个工作日内以书面方式明确不接受证书时视为拒绝。

4.4.3 订户接受证书的记录和保存

程远未来将根据交付方式的不同，在系统数据库中保存订户接受证书的信息。

保存内容包括：

- 1) 订户接受证书的时间和结果；
- 2) 订户接受证书的方式；
- 3) 订户接受证书的人员。

4.4.4 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证书策略保障的。

4.5.1 交付前的安全保护

订户的签名密钥不论是通过密码模块或由程远未来的私钥管理相关服务生成或采用通过主管部门认可的其他创新性保护方案，都处于安全的保护环境下。除上述三种签名私钥持有方式外，订户使用任何其它方式产生的签名私钥，程远未来都不予以认可。当程远未来根据订户申请，需要向订户交付加密密钥对时，在将密钥对交付订户保管之前，程远未来将采取有效措施保障其安全性，包括但不限于：

- 1) 保障加密私钥生成和传输过程的安全；
- 2) 审核订户密钥是否符合国家或行业相关安全标准要求，对不符合要求的（如 RSA 密钥长度小于 2048 位、使用 MD5、SHA-1 等不安全算法）拒绝颁发证书。

4.5.2 私钥管理服务

程远未来提供订户签名私钥管理服务，将采用科学专业的技术措施进行管理，并在此承诺：

- 1) 未经订户书面授权，不保存或委托他人保存其签名私钥；
- 2) 机构证书签名私钥的使用，会设置法定代表人或受托人作为授权主体；
- 3) 仅在获得订户明确授权的情况下使用其签名私钥；
- 4) 签名私钥会以加密形式存储，且存储条件符合安全标准；
- 5) 所有涉及签名私钥的操作会进行完整、可追溯的记录。

4.5.3 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。订户接收到数字证书后，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。

4.5.4 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，依赖方应独立地进行如下评估：

- 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。

4.5.5 安全事件反馈

程远未来建立便捷的外部安全事件反馈渠道，及时受理和处理证书信息错误、私钥失密或证书被盗用等异常情况。

4.6 证书续期

证书续期是指在不改变订户主体信息的情况下，在原证书到期前，为订户签发一张新的证书。续期后的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 证书续期的情形

- 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，向程远未来申请续期证书。对于过期的证书续期申请，程远未来将根据实际的安全需求决定是否允许续期。证书撤销后，将无法进行续期，只能按照初始流程重新申请证书。在证书密钥使用年限内，证书续期一般只延长有效期，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 请求证书续期的实体

订户可以请求证书续期。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 证书续期请求的处理

程远未来对请求证书续期的订户身份进行鉴别,确认续期请求是证书订户或订户授权的受托人提出的。

申请人为订户或其受托人,在受理续期请求时的身份查验方式为:若自申请人上次完成身份查验之日起至本次续期申请日未满三年,可使用有效的原证书进行电子签名验证的方式进行确认,否则,按照 § 3.2 的规定重新进行身份查验;证书签发与接受的流程按 § 4.3 与 § 4.4 的规定进行。

对于订户不能提供拟被续期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 构成接受续期证书的行为

同 § 4.4.1。

4.6.6 电子认证服务机构对续期证书的发布

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为订户生成新的证书密钥对并为其新公钥签发新证书的行为。证书密钥包括签名证书密钥和加密证书密钥。申请人为订户或其受托人。

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

证书变更是指改变证书中除订户公钥之外的信息而签发新证书的情形,例如:订户名称改变、其他有效证件号码改变情况。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、授权人信息等,可以向程远未来提出注册信息修改,无需证书变更。

申请人为订户或其受托人,按照 § 3.2 的规定查验,若发起方不是证书订户,程远未来须取得订户同意。

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),然后按照初次申请证书过程进行处理(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 证书撤销或冻结

4.9.1 证书撤销与冻结的审批流程

当程远未来接收到订户（含受托人）的撤销或冻结申请时，由相应的操作人员进行审批。审批时，程远未来需要检查撤销或冻结申请的证书是程远未来签发的、证书状态有效，操作人员需根据 § 3.1、§ 3.2、§ 3.3 等要求，确认订户的真实身份和真实意愿。审批通过后，才能进行证书撤销或冻结。

当程远未来接收到订户之外的其他依赖方发起的撤销或冻结申请时，由运营中心审批（包括审核报送的撤销材料及申请原因）。审批通过后对订户的证书进行撤销或冻结并通告证书订户。对于每月撤销原因为“CA 机构证书制作错误”达到 100 张的，需要上报相关主管机构。

4.9.2 可请求撤销或冻结的实体

根据不同的情况，请求撤销或冻结证书的实体，包括但不限于订户、受托人、依赖方、程远未来、司法机关等公共权力部门等。

4.9.3 请求处理

订户主动要求撤销或冻结自己的证书的，应告知程远未来进行撤销或冻结的原因（如密钥遗失或泄露等），并提供有效身份证明文件及证书撤销或冻结申请文件，并接受证书撤销或冻结申请的有关条款，同意承担相应的责任。机构订户撤销或冻结证书应由其授权的受托人提出申请。

订户可通过面对面、热线电话、电子邮件、传真、特快专递、网页等可靠的方式向程远未来提出证书撤销或冻结申请。收到订户的撤销或冻结申请及材料后，程远未来将根据 § 3.1、§ 3.2、§ 3.3 等要求，确认订户的真实身份和真实意愿，并确认订户需撤销或冻结的证书是否为程远未来所签发，证书是否在有效期内，

撤销或冻结材料及理由是否属实，若均通过则对证书进行撤销或冻结，并保留处理撤销或冻结流程的相关申请信息和处理信息。

当程远未来有充分的理由相信需要撤销或冻结订户的证书时，程远未来的有关人员可以通过内部确定的流程提请撤销或冻结证书。在证书撤销或冻结后，程远未来将通过适当的方式，包括邮件、传真、短信等，通知订户证书已被撤销或冻结及被撤销或被冻结的理由。

无论审批结果如何，程远未来均会向申请者反馈申请的受理情况（同意或驳回）并记录和保留本次申请、处理流程的相关信息。

4.9.4 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。

4.9.5 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，应及时向程远未来提出撤销请求。从发现需要撤销证书到向程远未来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。

4.9.6 电子认证服务机构处理撤销请求的时限

程远未来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。

4.9.7 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。

4.9.8 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。

4.9.9 CRL 发布的最长滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.9.10 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。

4.9.11 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。

4.9.12 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。

4.10 证书状态信息服务

程远未来通过网站 CRL、OCSP、LDAP 方式提供证书状态信息服务。

对于被撤销证书，其状态将同时在 CRL、OCSP 反映。

4.10.1 证书状态信息服务方式

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 提供客户端查询证书的当前状态；
- LDAP 提供客户端查询服务，证书目录符合 LDAP V3(RFC3377, 2251-2256, 2829-2830)。

4.10.2 证书状态信息服务响应时间

程远未来提供证书状态信息服务响应时间为不大于 3 秒。

4.10.3 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，订户能够实时获得连续不间断的证书状态查询服务，服务可用率不低于 99%。

4.10.4 备用查询方式

程远未来 CA 证书订户可通过官网和服务电话查询证书状态信息。

服务电话：023-67302734；电话服务时间：工作日 09:30-18:30，以此备用查询。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。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 停止使用认证服务

停止使用认证服务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。

停止使用认证服务包含以下两种情形：

- 1) 证书有效期满，订户不再进行证书续期、证书变更或者证书密钥更新，订户可以停止使用认证服务；
- 2) 证书在有效期内被撤销后，且订户没有进行证书变更或者证书密钥更新，即停止使用认证服务。

处理停止服务请求的时限和方式，包括：

- 1) 有效期满的证书，在有效期截止日期到达时即停止认证服务；有效期内被撤销的证书，在受理撤销业务后 2 个工作日内停止认证服务。当订户私钥由程远未来保管时，程远未来在受理撤销业务后 2 个工作日内采用安全的技术手段对订户签名私钥进行销毁。
- 2) 认证服务结束后，程远未来将对用户证书的相关数据保存至证书失效后 5 年；对用户资料的销毁参照《订户档案管理制度》进行；需转移用户资料时将依照国家相关政策。

停止服务后可能涉及的责任延续条款见 § 9 中法律责任和其他业务条款；

程远未来完整记录证书停止认证服务后的全过程操作情况。

4.12 密钥托管与恢复

程远未来的根证书私钥不会托管给任何第三方机构或个人，会在自身控制的安全环境中保管，同时建立根证书密钥备份与恢复策略，对根证书密钥进行安全备份。

4.12.1 密钥托管与恢复的策略与行为

程远未来的 CA 签名密钥安放于程远未来数据机房保管。

程远未来建立根证书密钥备份与恢复策略，对根证书密钥进行安全备份。

程远未来订户的签名密钥托管服务，签名密钥存放于程远未来数据机房/私有云保管，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；
- 国家其他管理部门行政管理需要。

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 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 基础设施

程远未来机房位于重庆市两江新区人和街道镜泊中路5号1栋1层。

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 分区管理和访问控制

程远未来实行分区域访问的安全管理策略。

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。四个功能区域按照安全级别逐级分层，为了保证系统的安全，采取了一定的隔离、控制、监控手段。机房设置门禁系统，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，并记录在动环监控系统中，每月对门禁记录进行整理归档。

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，设有电子门禁系统，授权人员采用指纹或密码验证方式进入。

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。

5.1.3 电力保障

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。

机房采用两路市电线路供电，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 跟市电独立工作，保证在市电供电出现问题时，UPS 也能正常启动工作。停电时，供电系统由 UPS 自动供电。

5.1.4 门禁与监控

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报警系统来重点保护机房物理安全。

物理访问控制包括如下几个方面：

- 1) 门禁系统：控制各层门的进出。工作人员需使用身份识别卡结合指纹鉴定才能进出，每一道门均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。
- 2) 报警系统：门禁系统设有门开超时报警，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。
- 3) 监控系统：根据机房动力环境监控系统的要求，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。

服务区的视频监控记录在硬盘录像机里保存，通过循环记录的方式保存 3 个月，门禁访问记录的保存时间为 3 个月。

管理区和核心区的视频监控记录在硬盘录像机里保存，通过循环记录的方式保存 6 个月以上，并单独对核心区机房视频监控记录进行循环备份保存。

门禁访问记录存在动环监控系统中，每月定期对门禁访问记录进行备份刻盘归档备查。

监控记录和门禁记录在销毁前进行安全审计，审计报告归档备查。

5.1.5 灾备

每月对网络、安全设备配置、数据库、官网等重要数据进行刻盘备份，并寄往北京进行异地备份保存。

异地备份位置为重庆程远未来电子商务服务有限公司北京分公司（北京市朝阳区青年路西里 3 号院 7 号楼 1 层 F1-49），距离重庆程远未来电子商务服务有限公司约 1500 公里。

5.1.6 环境保障措施

程远未来机房通过设置机房专用精密空调、新风系统、除湿机等设施，精准控制机房设施中的温度和湿度环境，保持湿度在 40%-60% 范围内，保持温度在 18° -28° 范围内。空调系统使用两台独立空调互为备份。

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。动环监控系统漏水监控子系统用于监测漏水情况，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。

5.1.7 消防措施

程远未来机房配备联动的火灾自动报警系统和自动灭火系统。按照国家相关法律法规的要求，每月定期进行维护保养，每年定期进行检测。

在公共区、服务区、管理区、核心区内各个位置根据相关要求设置烟感、温感探测器，通过消防火灾报警联动控制器进行管理，监控火警情况并进行处置。

核心区配置独立的气体灭火装置，使用七氟丙烷气体灭火系统，同时有两个隔绝式压缩氧气自救器。配置两个二氧化碳气体灭火器和过滤式自救呼吸器。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。

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。具有自动和手动两种触发装置方式。

火灾自动灭火设施的区域内，在隔墙上开孔加装甲级防火门。

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。动环监控系统与火灾自动报警系统设备联动，发生报警时，自动打开所有门。

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，关闭连锁设备，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。

5.1.8 设备管理

建立设备台账，设备台账包含每台设备的责任人、使用状态、维护周期和报废标准；定期进行设备盘点和核对，设备实际情况与设备台账相符；

程远未来制定了《固定资产及低值耐用品管理规定》，定期进行设备盘点和核对。

5.1.9 存储媒体管理

制定详细的存储媒体使用、报废管理规定，规定包含使用权限、报废标准、销毁方法和审批流程；完整记录存储媒体领用、归还、报废等情况。

程远未来制定了《移动存储设备管理规定》、《存储介质使用报废管理规定》，规定包含移动存储设备的责任人、使用权限、报废标准、销毁方法和审批流程，对设备的领用、归还、报废的做出了相应的记录。

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）。

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。

5.2 操作过程控制

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。相关可信角色包括：

1) 系统管理员

设置目的：

对本机构电子认证系统进行维护，协调和监督电子认证系统等基础设施正常运行，维护电子认证系统的完整性，保障电子认证系统的正常运转。

岗位职责：

- 系统策略配置、用户与权限管理。
- 加载系统根密钥、CA 证书、CRL、更新 CRL,配置系统，分配权限等。
- 配合制定运维的策略和流程，负责电子认证系统初始化、策略配置维护。
- 分析、评估并上报对电子认证系统的安全性有影响的改动。
- 负责电子认证系统逻辑访问控制的角色和相应的权限管理。
- 建立并维护与电子认证系统功能相一致的测试系统。
- 维护电子认证系统日志的完整性。

任职要求：

- 具有全面的计算机专业知识及系统管理经验，有计算机相关专业知识、PKI/CA 安全知识。
- 网络知识，操作系统知识，软件应用。
- 具有两年以上运维工作经验。
- 具有全面的计算机专业知识及系统管理经验。
- 具有风险管理能力,对安全体系有较深的认识,能够进行风险评估和管理,解决系统潜在的隐患或漏洞等风险。
- 有较强的领悟力和学习能力，擅长解决问题。
- 能够熟练使用主流的操作系统。
- 具备发现、处理问题的能力，工作认真细致、责任心强。

身份验证机制：指纹+IC 卡双因素认证+系统权限认证

最小人员配置：1 人

2) 技术运维员

程远未来对技术运维员进行了工作拆分，将技术运维员的工作划分为物理环境、网络和服务器等系统管理三个岗位，分别设置了物理环境管理员、

网络管理员和系统管理员三个角色。

a) 物理环境管理员

设置目的：

- 对本公司运营场地的门禁、监控、照明、电力、空调、消防、综合布线、静电防护、防雷、防灾等各项物理安全设施的日常监控与维护。
- 保障运营场所、机电基础设施正常工作。

岗位职责：

- 负责机电、门禁监控设备、消防设备等的管理及维护。
- 根据访问控制策略，制定和维护访问控制相关的管理办法和操作规程，管理本机构人员的物理访问权限及外来人员的访问控制。
- 编写和更新各项应急预案。
- 场地工程建设和改造维护。

任职要求：

- 机电、安全相关专业，持有电工特种作业操作证。
- 5年以上机电、安全等工作经验，具有1年以上建筑物、监控、消防方面的工作经验。
- 能够正确理解并运用《建筑设计防火规范》、《民用建筑电气设计规范》、《电子信息系统机房设计规范》等国家的相关安全技术规范和标准。
- 能够依据机电管理流程对机电等设备进行管理。
- 具有火灾、水灾防护等安全知识。

身份验证机制：指纹+IC卡双因素认证

最小人员配置：3人

b) 网络管理员

设置目的：

对本机构内外网络进行维护管理，制定网络策略.保障本机构网络的正常服务和IT设备的正常工作。

岗位职责：

- 负责网络设备和安全设备的运维管理，确保各系统网络处于安全、稳定运行状态。
- 正确配防火墙，测试防火墙策略的有效性，保护 CA 内部网络域，防止未授权的访问。
- 正确配置电子认证系统和办公系统的网络访问。
- 对提供的服务（如 HTTP、FTP 等）进行正确配置，停止不需要提供的服务进程，关闭不需要使用的端口，使用路由控制和安全通道保护外部远程电脑访问。
- 建立检测和防护控制来防止病毒和恶意软件，并能提供适当的报警信息。
- 制定运维策略和流程，建立并执行网络系统故障报告、处理流程。
- 分析网络入侵事件日志，及时响应安全事件，调整安全策略。

任职要求：

- 计算机相关专业，具有信息安全相关认证资质。
- 2 年以上计算机网络安全管理经验。
- 具有大中型机房网络系统、服务器系统运维、实施相关经验。
- 熟悉主流厂家各系列防火墙、路由器、交换机等设备的配置操作。
- 熟练掌握负载均衡，IDS/IPS，WAF 等设备的工作原理及配置，具有丰富的系统集成经验。
- 熟练掌握计算机网络技术，深刻理解 TCP/IP 协议、交换和路由协议。
- 能够正确运用计算机专业知识、PKI/CA 安全专业知识。
- 能够正确运用网络安全策略。
- 有较强的领悟力和学习能力，擅长解决问题，工作细致。

身份验证机制：指纹+IC 卡双因素认证+网络管理系统身份认证

最小人员配置：1 人

c) 系统管理员

设置目的：

- a) 负责对本机构办公系统、电子认证系统进行维护，协调和监督电子认证系统和运营物理环境等基础设施正常运行，维护系统的完整性，

保障系统正常运转。

- b) 对系统架构及涉及的软件进行维护管理优化、升级。
- c) 制定相关安全策略，保障系统安全，确保基础环境的稳定运行。

岗位职责：

- 服务器硬件故障的排查及维护，建立并执行服务器系统故障报告、处理流程。
- 定期检查系统及网络的稳定性、安全性及容量是否符合服务水平。
- 建立监控流程，确保记录并报告发现的或怀疑的、对系统或服务有威胁的安全缺陷。
- 建立并执行系统故障报告、处理流程。
- 监控电子认证系统的操作系统、备份系统的软硬件的正常运行，及时发现并排查故障。
- 分析、评估并上报对服务器系统的安全性有影响的事件。
- 配合制定运维的策略和流程，并按照要求对系统进行安全优化等。
- 负责公司网站的发布和维护。
- 负责系统日志的分析及相关备份。

任职要求：

- 熟悉 Windows/ Linux 服务器操作系统部署与维护以及安全配置。
- 熟练掌握 Windows/ Linux 下 Web 应用架构，能够熟练配置及优化 Web 服务器。
- 熟悉网络技术，具备基本的网络相关知识。
- 熟悉主流开源监控系统（如 Zabbix/Cacti）。
- 具有计算机专业知识、PKI/CA 安全知识要求。
- 具有两年以上 Linux 操作系统运维经验。
- 具有一定的计算机专业知识及系统管理经验。
- 能够根据网络安全需求，确保系统安全。
- 具有风险管理能力，对安全体系有较深的认识，能够进行风险评估和管理，解决系统潜在的隐患或漏洞等风险。
- 有较强的领悟力和学习能力，擅长解决问题。

- 能够熟练使用主流的操作系统。

具备发现、处理问题的能力，工作认真细致、责任心强。

身份验证机制：指纹+IC 卡双因素认证+操作系统身份认证

最小人员配置：1 人

3) 数据库管理员

设置目的：

保障本机构数据库管理系统的稳定性、安全性、完整性和高性能，确保数据库系统的正常运行。

岗位职责：

- 负责数据库系统部署方案的计划、设计、实施和管理维护。
- 负责对数据库的运行状态，日志文件，备份情况，数据库的空间使用情况，系统资源的使用情况进行检查，发现并解决问题。
- 负责对数据库对象的空间扩展情况，数据的增长情况进行监控，对数据库做健康检查，对数据库对象的状态做检查。
- 负责对表和索引等进行分析，检查表空间碎片，进行数据库性能调整。
- 负责保障数据安全和稳定可用。
- 负责数据库备份管理、监控备份情况，应急恢复策略方案的制定与实施。
- 为开发人员提供数据库技术支持，如数据库迁移、测试库安装及数据导入等。

任职要求：

- 计算机、数学及相关专业。
- 具备 3 年以上大型数据库管理经验。
- 熟悉主流的关系型数据库，具备丰富的 ORACLE、MySQL 等数据库 DBA 工作经验。
- 熟悉数据库设计、管理、性能调优及备份恢复等日常工作，能独立完成数据库管理维护工作。
- 具有根据业务发展情况设计系统存储备份、灾难恢复方案的能力。

- 熟悉 UNIX、LINUX 等操作系统，能够独立完成数据库的安装、备份、恢复和调优，并能够编写 shell、python 脚本。
- 具有计算机专业知识、PKI/CA 安全专业知识。
- 拥有良好的沟通表达能力和服务意识，有较强的团队合作意识，快速处理系统突发事件的能力。

身份验证机制：指纹+IC 卡双因素认证+系统权限认证

最小人员配置：1 人

4) 系统审计员

设置目的：

定期对系统和网络日志进行安全审计和管理并生成审计报告，负责对涉及系统安全的事件、各类管理和操作人员的行为进行审计和监督，确保遵从法律和法规，降低运营风险，提高服务质量，保证运营的可持续性。

岗位职责：

- 检查法律和法规方面的符合性，运营是否符合安全策略、证书策略、认证业务规则等。
- 评估服务能力和运营安全性，是否在人力资源、运营管理、技术、安全管理、财务等方面存在风险。
- 向安全策略管理组织提交审计报告。
- 对审计中发现的问题进行跟踪并直至解决。

任职要求：

- 熟悉相应网络安全政策。
- 具有两年以上运营审计相关工作经验。
- 能够对涉及系统安全等事件进行审计。
- 能够对服务和运营风险进行正确评估。
- 具有良好的表达能力和沟通能力。

身份验证机制：指纹+IC 卡双因素认证+智能密码钥匙身份认证

最小人员配置：1 人

5) 密钥管理员

设置目的：

- 负责负责根证书密钥材料管理负责对电子认证私钥和证书的生命周期进行维护，及相关密码设备进行管理和操作。
- 维护电子认证私钥的物理安全和逻辑安全，确保所创建私钥和证书的完整性和可审计性等。

岗位职责：

- 为程远未来创建并维护电子认证密钥对和证书。
- 与相关部门协作，贯彻电子认证密钥对的物理和逻辑安全要求，确保电子认证密钥生成规程的完整性和可审计性。
- 保证按期、按需、安全地完成根密钥生成仪式的准备、实施及善后工作。
- 确保服务器密码机的安全性，及初始化前后的维护和保管工作。
- 积极配合相关部门的工作，包括系统维护的电子认证密钥等。
- 严格执行密钥管理的各项规章制度。
- 建立当电子认证私钥可信性受威胁时的应变计划。
- 保证与密钥管理相关的机密文件的安全保存。
- 与密钥分管者共同保管好所有根密钥相关物品和文档资料。
- 协助电子认证私钥的恢复工作。
- 制定用户加密密钥查询和恢复管理策略和流程，配合获得授权的国
家机构以规定的方式进行密钥查询和恢复。

任职要求：

- 英语听说读写良好，具有计算机网络安全、信息安全技术等相关专业，对 PKI/CA、加密技术有基本的了解。
- 有 5 年以上计算机相关工作及组织协调类工作。
- 能够遵照国家的各项安全技术规范和标准对密钥进行管理。
- 能够正确使用本机构的加密设备。
- 具有一定的应急处理能力，能够对突发事件进行及时处理。
- 诚实、可靠；对工作认真、细心；具有团队合作意识。

身份验证机制：指纹+IC 卡双因素认证+智能密码钥匙身份认证

最小人员配置：3 人

6) 业务操作员

程远未来将证书受理业务细分为三个岗位：业务咨询岗、业务受理岗和鉴证岗，对应设置了业务咨询员、业务受理员和鉴证服务员三个角色。

a) 业务咨询员

设置目的：

- 向用户提供电子认证服务业务介绍、业务办理流程、证书应用和电子认证服务相关法律法规的解读。
- 针对服务订户在业务办理前、业务办理中的各种需求，以及证书应用过程中的各种使用需求提供咨询服务。

岗位职责：

- 熟练掌握公司电子认证业务规则和相关制度，熟练准确向用户解答证书业务的各类咨询和相应服务流程。
- 对证书应用业务的咨询应提供相应的专业的知识解答。
- 对电子签名法相关法律条文的咨询能明确解答。
- 明确告知申请者和电子认证服务提供者的责任与义务。

任职要求：

- 具有基本的 PKI/CA 知识、数字证书应用知识及计算机网络基本知识。
- 能够熟悉并正确理解《电子签名法》、《电子认证服务管理办法》等法律法规。
- 3 年以上客户服务工作经验，1 年以上电子认证行业工作经验。
- 熟练使用计算机及各种通用办公软件。
- 能够根据电子认证相关产品、系统的原理，确认客户需求，正确操作证书应用、基本问题解答。
- 良好的语言表达能力、客户导向、人际交往能力和学习能力。
- 具有一定的应急处理能力，能够对突发事件进行及时处理。

身份验证机制：指纹认证+智能密码钥匙身份认证

最小人员配置：1 人

b) 业务受理员

设置目的：

针对证书订户提供包括证书申请、证书签发、证书更新、密钥更新、证书变更、证书撤销、证书有效性验证、密钥生成、备份和恢复等在内的各种服务。

岗位职责：

- 证书业务受理，接收并初审客户申请材料，录入申请信息，制作证书并交付客户。
- 提供业务受理服务，具体包含：证书申请、证书签发、证书更新、密钥更新、证书变更、证书撤销和挂起，证书有效性验证、密钥的生成、备份和恢复、证书补办、证书口令解锁等。
- 开收据，定期整理客户申请材料，按规定时间移交档案管理员。

任职要求：

- 具有基本的 PKI/CA 知识、数字证书应用知识及计算机网络基本知识。
- 能够熟悉并正确理解《电子签名法》、《电子认证服务管理办法》等法律法规。
- 1 年以上客户服务或相关工作经验，1 年以上电子认证行业工作经验。
- 熟练使用计算机及各种通用办公软件。
- 能够根据电子认证相关产品、系统的原理，确认客户需求，正确操作证书应用、基本问题解答。
- 良好的语言表达能力、客户导向、人际交往能力和学习能力。

身份验证机制：指纹认证+智能密码钥匙身份认证

最小人员配置：2 人

c) 鉴证服务员

设置目的：

- 电子认证服务机构在业务办理过程中，对证书订户的身份真实性，过程真实性进行鉴证，以及对证书订户资料进行规范管理服务。
- 确认客户身份以及申请机构的真实性；确认客户证书服务请求的真实性；确保证书签发给正确的实体。

岗位职责：

- 执行公司电子认证业务规则中鉴证服务要求、原则，依照部门鉴证相关制度规定、流程开展服务工作。
- 对证书申请者的身份和其他属性进行鉴证，通过对用户提交的资质文件进行认证，以确认证书申请者的真实身份，同时对客户提交的申请信息进行确认
- 对申请办理证书业务的人员进行身份关联鉴证和行为鉴证。
- 对鉴证资料进行收集、备案、归档和查询。
- 不断探索学习鉴别验证服务相关知识，持续完善多种鉴证服务手段，提升工作效率和效果。

任职要求：

- 具有基本的 PKI/CA 知识、数字证书应用基本知识及计算机网络基本知识。
- 能够熟悉并正确理解《电子签名法》、《电子认证服务管理办法》等法律法规。
- 能够根据电子认证相关产品、系统的原理，正确操作证书应用、基本问题等解答。
- 1 年以上鉴证服务工作经验，1 年以上电子认证行业工作经验。
- 对于证书体系有深刻认识，理解证书服务的本质内容。
- 熟练使用计算机及各种通用办公软件。
- 具有基本的法律常识和较强的风险意识。
- 良好的沟通能力、分析判断能力、团队协作能力、解决问题能力和计划执行能力。

身份验证机制：指纹认证+智能密码钥匙身份认证

最小人员配置：2 人

7) 客户档案管理员

设置目的：

执行公司档案管理制度，保管公司所有档案，定期整理检查档案。

岗位职责：

- 负责建立和维护客户档案资料，包括客户提交的鉴证资料、各项服

务记录、服务协议及授权书等。

- 负责管理公司机房、运维、审计等工作开展产生的各种验收报告，记录资料、光盘说明书等，依照档案管理制度进行编号存档。
- 定期盘点检查档案资料，更新台账，维护档案资料的安全与整洁。
- 执行档案管理制度，负责借阅、查询、归还相关手续。

任职要求：

- 具有档案管理基础知识和工作经验。
- 具有基本的 PKI/CA 知识、数字证书应用基本知识。
- 能够熟悉并正确理解《电子签名法》、《电子认证服务管理办法》等法律法规。
- 能够正确操作证书应用、基本问题解答。
- 良好的沟通能力、分析判断能力、保密意识、团队协作能力和计划执行能力。

身份验证机制：指纹+IC 卡双因素认证+档案管理系统角色权限认证

最小人员配置：1 人

8) 运营审计员

设置目的：

定期对电子认证系统进行安全审计，负责对涉及业务的各类管理和操作人员的行为进行审计和监督，确保遵从法律和法规，降低运营风险，提高服务质量，保证运营的可持续性。

岗位职责：

依据包括电子认证服务机构发布和制定的所有与运营相关的安全策略、证书策略、电子认证业务规则等，以及国家法律法规和行业相关标准，对以下内容进行审计，并根据审计结果撰写审计报告和改进意见：

- 检查法律和法规方面的符合性，运营是否符合安全策略、证书策略、认证业务规则等。
- 评估服务能力和运营安全性，是否在人力资源、运营管理、技术、安全管理、财务等方面存在风险。
- 向安全策略管理组织提交审计报告。

- 对审计中发现的问题进行跟踪并直至解决。

任职要求：

- 熟悉相应网络安全政策。
- 具有两年以上运营审计相关工作经验。
- 了解运营业务的各项制度、流程和系统。
- 能够对服务和运营风险进行正确评估。
- 具有良好的表达能力和沟通能力。

身份验证机制：指纹+IC 卡双因素认证+智能密码钥匙身份认证

最小人员配置：1 人

9) 其他人员

为更好地服务公司运营，除了安全策略委员会负责人外，程远未来还设置了安全经理、财务经理、可信人员管理、法律事务、服务质量管理员等多个角色。

a) 安全策略委员会负责人

设置目的：

协调公司内部的运营管理人员、客户服务人员、服务管理人员等，组建安全策略管理组织，并进行 CPS 管理、监督执行，评估机构运营风险，应对突发情况管理，依法对 CPS 进行管理和监督执行。

岗位职责：

- 组建公司安全策略管理组织，并领导该组织工作。
- 负责定期组织修定和维护公司 CPS，并监督执行。
- 有效控制公司运营风险，保证电子认证服务质量和业务连续性。
- 安全策略委员会委员的免职以及任命。
- 组织制定技术策略和运营策略。

任职要求：

- 精通密码学及 PKI/CA 技术，CA 行业知识。
- 能够正确理解《电子签名法》、《电子认证服务管理办法》等法律法规。
- 具有 5 年以上的电子认证行业或相关行业高级管理工作经历。

- 能够理解电子认证服务机构、证书订户、证书依赖方权利和责任的规定。
- 能够正确理解电子认证方面的法规、规章和行业政策。
- 能够正确理解本公司制定的 CPS。
- 掌握电子认证事故应急救援预案程序。
- 能够制定信息安全管理方针和策略。
- 能够正确采用风险管理的方法进行信息安全管理计划、实施、评审检查和改进。
- 具有较强的组织协调能力、沟通能力、文笔功底较强。

身份验证机制：无

最小人员配置：1 人

b) 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。

设置目的：

对本机构运营场地安全、人员安全、信息系统安全、通信系统安全、及重要 IT 资产安全进行日常监控和审计监督。

岗位职责：

- 制定运营场地安全策略，包括物理访问控制、电脑终端的安全接触、电力空调等设备的安全使用。
- 制定人员安全策略，包括定义接触电子认证系统的各类安全角色和岗位、职责分割原则和权限控制机制，定期检查物理访问权限和逻辑访问权限的设置情况。
- 对电子认证系统各类安全事件进行分级，建立各类安全事件报告、跟进策略及处理机制的应急响应计划，并定期测试、评估和更新此计划的内容。
- 制定通信安全管理策略、变更申请和批准流程。保证通信系统的可靠性，预防通信系统泄露信息，防止非授权使用通信系统。
- 对记录认证机构涉及运营条件和环境、密钥和证书生命周期管理的

日志和事件进行监控。

- 控制各类介质包括光盘、硬盘、软盘、移动储存介质等，防止被盗、毁坏、被修改、信息泄露、未授权访问等情况发生。
- 对当前的安全策略和管理程序进行风险评估，并上报安全策略管理组织。
- 制定风险管理策略，对涉及运营的各类风险进行分析、评估和分级，并提供解决办法。
- 定期对相关人员开展安全培训。

任职要求：

- 具有信息安全相关认证资质。
- 能够正确的运用计算机网络、信息系统、PKI/CA 知识实现信息安全管理。
- 具有 2 年以上机房安全管理工作经验、场地维护经验。
- 熟悉 ISO27001 管理体系、电子签名法、国家相关运营管理法规、标准等安全相关规范。
- 能够对电子认证服务安全隐患排查及事故防范。
- 能够对电子认证事故进行应急救援和预案程序。
- 能够对机房运营安全制定相应的策略。
- 能够指导相关人员进行相关培训。
- 良好的组织协调能力、分析判断能力、决策能力。

身份验证机制：无

最小人员配置：1 人

c) 财务经理

设置目的：

- 管理公司的财务会计系统的日常帐务处理，报税指导，定期与客服部收款结算人员进行证书费用结算。
- 管理会计系统的统计和分析工作。
- 保证公司基本财务流程正常运行。
- 保证公司财务职能正常发挥。

- 提出账务工作及财务管理制度流程的改进思路 and 措施。
- 对公司的财务进行综合管理和风险评估，依法对电子认证服务机构的财务进行管理和风险评估，降低财务风险和机构运营风险。

岗位职责：

- 全面支持公司建账和账务调整工作。
- 凭证审核、入账、结账等基本账务工作。
- 负责公司成本核算。
- 编制财务报告，对机构的财务保障能力进行正确评估。
- 财务制度的建立、更新和监督指导。
- 组织编制机构年度综合财务预算和控制。
- 财务、税务政策的收集整理，财务档案管理。
- 负责管理会计的基础数据统计和分析工作。
- 政府立项的财务工作部分（申报、年检、验收审计）。

任职要求：

- 精通会计、财务相关专业。
- 3 年以上财务相关工作经验。
- 能够依照国际财务会计法规条例办理会计事务。
- 能够独立进行全盘帐务处理，合并报表和机构账务经验，熟悉税务流程；能够及时准确地对公司风险评估，降低财务风险和机构运营风险。
- 熟练使用财务软件，熟练使用各种办公软件。
- 拥有良好的执行能力和学习能力，关注细节、成本意识、沟通能力，承受压力，团队合作。

d) 可信人员管理

设置目的：

- 完善公司的薪酬、绩效、员工关系管理；实现公司员工激励，提高工作效率。
- 公司可信人员管理；提升公司人力资源效率；建立匹配公司发展战略的人力资源计划。

- 依据可信人员策略对公司各关键岗位、重要岗位、一般岗位人员进行人员管理，包括建立可信人员的管理制度、流程和规范，进行背景调查、入职、培训、上岗、转岗、离职等管理。

岗位职责：

- 建立可信人员策略，包括岗位可信人员要求、背景调查和程序。
- 在正式聘任员工授权接触公司重要资料前，证明其可信性，并签署员工保密协议。
- 建立每个工作岗位的工作范围及其责任，并确定关键岗位、重要岗位、一般岗位等不同岗位的可信要求。
- 建立和完善可信人员培训制度、人力资源管理制度，提出改进建议并制定相关改进方案。
- 建立可信人员异动管理制度，可信人员离职后应立即删除其接触公司资料的权限。
- 建立可信人员清单及所有人员清单。
- 劳动关系管理（入职、离职、解聘、背景调查、转正、续签、员工档案等）。
- 工资、福利管理（工资核发、保险、住房公积金、补助等）。
- 参与制定公司的绩效考核评估体系并组织实施各部门的绩效考核工作。
- 严格执行公司的各项人力资源管理制度同时做好关联部门的公共关系维护。

任职要求：

- 人力资源、劳动经济等相关管理类专业。
- 人力资源管理 2 年以上工作经验。
- 熟悉国家有关劳动、社保、人事的政策法规。
- 较强沟通能力、分析判断能力和员工关系管理能力。
- 良好的独立策划能力、沟通技巧、组织协调能力、分析判断能力和团队合作精神。

e) 法律事务

设置目的：

提供法律相关内容的解读、咨询，提供电子认证服务相关的法律事务支持。

岗位职责：

- 提供电子认证服务法律合规性保障。
- 向客户讲解分析《电子签名法》等法律法规。
- 向客户提供法律咨询和司法协助。
- 负责法律风险防范，构建法律风险防范体系，及时对法律风险进行预警、分析和建议。
- 负责对法律纠纷的处理。

任职要求：

- 法律专业，具有专业律师资格证。
- 能够正确理解《电子签名法》等法律法规中对电子认证服务机构、证书订户、证书依赖方权利和责任等内容。
- 能够正确理解电子认证服务机构运营体系。
- 能够独立起草、修改合同及法律文书。
- 能够独立承担纠纷诉讼案件。
- 能够恰当处理各种社会关系的能力。
- 具有良好的语言表达能力和文字表达能力。

f) 服务质量管理员

设置目的：

- 建立宣贯和持续改进程远未来质量管理体系。
- 监督提供电子认证服务的各岗位职责和行为规范的执行，并对服务环节涉及的业务过程，提出改进意见。
- 保证和提升产品和服务的质量。
- 按时提供质量管理报告。

岗位职责：

- 创建和完善技术咨询、客户服务、认证服务、项目实施、应用研发相关环节的质量管理体系。

- 对业务工作流程及结果进行检查和监督。
- 对业务咨询服务岗位、业务办理岗位、鉴证服务、技术支持服务岗位的职责规范进行质量跟踪和管理。
- 进行用户满意度调查，接受与处理用户投诉。
- 综合分析质量管理信息，提交质量管理报告，不断完善质量管理标准。

任职要求：

- 具有基本的 PKI/CA 知识、数字证书应用知识和计算机网络知识。
- 熟悉《GB/T 35289-2017 信息安全技术电子认证服务机构服务质量规范》等电子认证相关的法律法规和质量体系规范。
- 4 年以上 IT 行业工作经验，3 年以上管理经验。
- 具有良好的写作能力和口头表达能力、沟通能力、执行能力
- 具备良好的人际交往能力、团队合作能力、成本意识、解决问题能力
- 具有结果导向意识和成本意识。

g) 技术支持服务

设置目的：

在提供电子认证服务时提供技术支持，为解决订户在证书使用过程中的各种技术问题和电子认证系统故障提供技术支持服务。

岗位职责：

- 主要解决证书使用问题和认证服务系统故障两大方面问题，包括数字证书管理、数字证书使用、证书存储介质硬件设备使用。电子认证系统使用以及各类数字证书应用（如：证书登陆、证书加密、数字签名）等。
- 明确对一般事件、严重事件、重大事件的处理流程和响应时间，以最大程度不影响客户使用为准则；形式上采用电话支持、远程协助支持、现场支持。
- 及时准确向上级反映服务过程中的问题，客户的需要，提交合理化建议等。

任职要求：

- 具有基本的 PKI/CA 知识、数字证书应用基本知识及计算机网络基本知识。
- 能够熟悉并正确理解《电子签名法》、《电子认证服务管理办法》等法律法规。
- 能够根据电子认证相关产品、系统的原理，正确操作证书应用、基本问题等解答。
- 1 年以上客服售后相关工作经验, 1 年以上电子认证行业技术支持相关工作经验。
- 能够使用至少一种通用的开发语言、至少 2 种通用的数据库、一种 web 服务器、一种通用的操作系统。
- 良好的沟通能力、分析判断能力、团队协作能力、解决问题能力和计划执行能力。

h) 产品研发

设置目的：

顺应客户需求，完善电子认证服务的产品线，负责研发公司主营产品或升级，提高电子认证服务的层次和水平。

岗位职责：

- 电子认证服务产品、系统的研发。
- 电子认证服务产品、系统维护和升级。
- 支撑项目实施人员完成实施任务。

任职要求：

- 具有计算机相关专业知识、PKI/CA 安全专业知识。
- 2 年以上技术研发相关经验，1 年以上软件项目管理经验。
- 能够使用至少 2 种开发语言和相关开发工具，擅长 Eclipse、IDEA 等 IDE 使用开发技巧和调试技巧。
- 具有使用通用的开源框架的能力和经验。
- 能够使用主流的数据库进行设计开发。
- 能够正确理解国内各项安全规范和标准。

- 能够正确理解电子认证方面的法律、法规和规章制度。
- 具备良好的团队合作精神和高度的责任感，对工作积极严谨，勇于承担压力。
- 具备良好的英语阅读能力，能够正确阅读岗位所需知识的英文文档。
- 拥有新技术的学习能力，创新精神。

i) 项目实施

设置目的：

负责安装、配置公司各类 CA 产品。降低电子签名技术难点，为电子签名人提供完整的技术支持和服务，提高客户满意度。

岗位职责：

- 负责 CA 产品各种版本的安装、配置和修改，解决项目实施过程中的突发问题。
- 负责公司各种证书应用软件以及各种版本证书 API 的使用，并不断完善各种版本证书 API。
- 负责对客户进行公司产品和 PKI/CA 培训。
- 解决项目中突发的各种问题，现场进行系统安装、部署和测试。
- 提供相关的系统培训。

任职要求：

- 具有计算机相关专业知识、PKI/CA 安全专业知识。
- 2 年以上 IT 行业工作经验，1 年以上软件项目管理经验。
- 能够正确理解电子认证方面的法律、法规和规章制度。
- 擅长任意高级计算机语言和 C/C++，精通 HTML 及脚本语言开发。
- 具备数据库基础知识。
- 具备网络基础知识。
- 精通 Windows，熟练使用 Linux/Unix 及开发。
- 有良好的英文文档阅读能力，能够正确阅读岗位所需知识的英文文档。

本机构所有岗位不少于 1 人。业务办理不少于 2 人，系统维护不少于 2 人，物理环境不少于 3 人，鉴证服务不少于 2 人。其他岗位人员数量根据业务发展需

要设置。

在执行以下操作前，程远未来对服务于相关岗位的人员进行鉴别。

- 1) 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；
- 2) 对进入机房区域的人员分配门禁卡并录入指纹；
- 3) 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 UsbKey 的数字证书。

身份鉴别包括：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相关要求进行。

5.2.2 职责分离

本机构遵循职责分离原则，所有涉及关键操作(密钥管理、审计、鉴证、系统管理)的角色均实现双人操作或复核机制：涉及业务连续性相关操作(运维、鉴证、审计等)的角色按工作量设置人员冗余，在任何一人缺岗时仍能实现双人操作；禁止同一人员掌握可独立完成“发起、审批、执行、审计”全流程的任何组合，以下角色禁止相互兼任：

- 1) 系统管理员、技术运维员、数据库管理员、系统审计员之间不兼任；
- 2) 同一证书业务的录入与审核环节不由同一业务操作员完成；
- 3) 业务操作员、客户档案管理员、运营审计员之间不兼任；
- 4) 密钥管理员不与系统管理员、技术运维员兼任；
- 5) 密钥管理员不与除策略管理机构成员外的其他可信角色兼任。

5.3 人员控制

5.3.1 可信人员资格要求

所有的员工与程远未来签订具有法律约束力的保密协议和劳动合同，并承诺不得私自保存、复制或泄露电子认证服务的所有秘密或敏感信息。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

历专业技能应足够胜任其工作，对其从业经历会进行调查记录。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、无犯罪记录等。

5.3.2 可信人员培训要求

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岗前培训，对所有在职员工安排持续的定期培训，对从事销售、服务和支持相关岗位的人员安排符合其岗位需求的专业培训，建立覆盖所有可信角色的持续培训体系。

培训类型分为岗前培训和持续培训。岗前培训为所有可信人员上岗前须完成不少于 20 学时的培训并通过考核；持续培训为每年至少接受一次培训，每人每年培训时长不少于 20 学时，并通过考核。

培训内容包括但不限于：

1) 《电子认证服务管理办法》、《电子签名法》和《GB/T 35288-2017 信息安全技术 电子认证服务机构从业人员岗位技能规范》等电子认证服务相关的法律法规与标准；

2) 岗位职责要求及各角色特定的工作要求；

3) 内部管理政策、规章制度、工作流程、办公应用软件、操作系统与网络等；

4) PKI 和密码技术的基础知识；

5) CPS、CP；

6) 安全管理策略要求和机制；

7) 订户身份查验和审核策略和流程；

8) 电子认证服务运营体系构成；

9) 电子认证服务技术体系构成；

10) 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；

程远未来每年会对培训内容进行审查修订。

5.4 审计日志程序

5.4.1 记录范围

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

5.4.2 记录内容

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时间、类型、内容、操作人、作用对象及结果。对系统的关键操作由操作人员进行电子签名等。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。

5.4.3 保存期限

系统日志至少保存至相关证书失效后五年，并实施严格的访问控制以防篡改或删除。

对于电子审计信息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,则有专门的文件档案柜用于审计信息的保存,纸质的审计文件由档案管理员进行保管。

5.4.4 日志审计内容

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

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 审计周期

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

5.4.6 审计日志备份程序

程远未来保证所有的审计记录和审计总结每周进行备份。

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。

5.4.9 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。

5.5 记录归档

5.5.1 归档范围

- 1) 证书申请材料和订户意愿记录;
- 2) 所有审计日志;
- 3) 密码设备全生存周期管理记录;
- 4) 密码设备的日常操作与使用记录;
- 5) 根证书或密钥生存周期管理相关的全部记录;
- 6) 证书认证系统运行日志;
- 7) 已识别的安全事件及处置记录;
- 8) 证书认证系统关键操作日志;
- 9) 电子认证服务过程中其他操作记录;
- 10) 已失效的订户和 CA 公钥证书文件。

5.5.2 保存期限

订户相关档案、系统日志和审计记录至少保存至证书失效后五年:

- 1) 对订户证书生命周期内的管理事件的归档,至少保存至证书失效后 5 年;
- 2) 对 CA 证书和密钥生命周期内的管理事件的归档,至少保存至证书失效后 5 年;
- 3) 订户证书的资料和公钥证书归档至少保存至证书失效后 5 年;
- 4) 对于所有的审计记录的归档,至少保存至证书失效后 5 年;
- 5) CA 证书和密钥的归档在 CA 证书和密钥生命周期之外,至少保存至证书失效后 5 年。

5.5.3 保护措施

对电子归档记录采取技术手段保障其完整性,并存储在安全的物理与数字环境中,建立备份机制。

程远未来的存档内容有物理安全措施的保证,电子存档内容应用了密码技术做保护。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。

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记录事件/日志进行相应操作。记录事件/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。记录事件/日志的制作和访问进行岗位分离。

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。

5.5.4 归档记录管理

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,并建立了档案管理制度,明确了管理职责、操作规范和安全要求。

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。

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。

5.5.5 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。

5.6 电子认证服务机构根证书密钥更替

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。

5.6.1 密钥更替程序

当 CA 密钥对即将达到最大生命期时，程远未来启动 CA 密钥更新流程，替换即将过期的 CA 密钥对。CA 密钥变更按如下方式进行：

- 1) 密钥生成：在颁发或更换根证书时，在安全可靠的环境中生成新密钥对，按照 § 6.2.1 进行相关操作；
- 2) 根证书发布：将新的 CA 公钥证书发布给证书订户和依赖方；
- 3) 旧密钥处理：在完成签名密钥更替后，程远未来将按 GB/T 25056—2018 中 8.2.4.3 规定的方式，销毁旧私钥及其备份，并保留相关操作记录。

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。

5.6.2 密钥更替的时间

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

5.7 损害和灾难恢复

5.7.1 业务连续性目标

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：

- 1) 认证系统应急方案；
- 2) 动力系统应急方案；
- 3) 消防应急方案；
- 4) 网络与信息系统应急方案；
- 5) 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。

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集群部署方式；对核心数据库，有本地及异地备份机制。

程远未来承诺灾难恢复时间目标（RTO）为 24 小时内，恢复点目标（RPO）为 24 小时内。

5.7.2 恢复流程

1) 证书库的恢复过程：

程远未来证书库采用数据库记录存储订户的证书信息及撤销的证书列表信息。为保证证书库快速恢复，程远未来的证书数据库使用双机主从备份（数据库硬件配置相同）和使用虚拟 IP（所有应用均指向数据库的虚拟 IP），同时添加了对数据库的相关监控，实现数据库访问异常的实时报警。当主库出现异常且判断暂时无法快速解决问题时，可根据《认证系统应急方案》等指引，快速完成主备库切换。

程远未来对认证系统实现了多节点部署方案并使用轮询检测机制，当检测到某个签发服务异常时，可直接从服务列表中移除。

使用数据库主从备份和多节点部署应用的方式，可降低重建安全运行环境的复杂性，减少系统应用恢复时间，对证书列表、证书私钥重新快速向订户提供实

体公钥证书服务不会造成明显影响。

根密钥损害的恢复过程：

密钥管理员得到授权后，在 CA 机房执行如下操作：

- a) 联系相关管理人员，获取密码机连接专用设备（笔记本）
- b) 召集三名及以上的密钥分管员，进入 CA 机房，分别从密钥保管箱中取出密钥备份 U 盘和 IC 卡；
- c) 使用专用设备连接服务器密码机；
- d) 在专用设备上插入密钥备份 U 盘，使用专用设备上的专用恢复程序打开密钥备份 U 盘；
- e) 在专用设备上输入密码机的相关信息（IP 地址、用户名和密码）；
- f) 各密钥分管员根据专用恢复程序提示分别插入自己的 IC 卡，直至程序提示密钥恢复完成；
- g) 重启密码机，确认根密钥恢复成功；
- h) 全程摄像并上报。

其他关键资产恢复过程：

程远未来对包括其他关键资产，如 CA 物理设施、计算资源、网络环境、软件或数据，以及其他密钥数据等均制定了相应的恢复方案，一旦出现对应的问题可根据相应方案进行恢复。这些应急处理方案有：

- ①认证系统应急方案；
- ②动力系统应急方案；
- ③消防应急方案；
- ④网络与信息系统应急方案；
- ⑤安全事故应急处理方案等；

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、软件或数据的损坏时，会在最短的时间内恢复被损害的资源、软件或数据。

5.7.3 根私钥应急处理

程远未来建立了根私钥泄露应急处理流程，流程明确了应急响应时间要求、责任人员、处置步骤和上报机制，每年进行一次应急演练。

当订户证书私钥发生泄露时，按照证书撤销和挂起流程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，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 事件报告

程远未来严格按照 § 5.9 相关要求进行事件报告。

5.7.5 定期验证

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

5.8 电子认证服务机构终止

当程远未来因技术性原因或商业原因需要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，具体流程和通告机制包括但不限于：

- 1) 起草并发布 CA 终止声明，至少提前九十日通知与证书订户、依赖方等相关实体，至少提前六十日向主管部门报告；
- 2) 具有资质的电子认证服务业务承接单位，并签署承接协议，明确约定承接机构的工作范围与责任；
- 3) 向承接方移交密钥及相关关键数据，协调承接单位启动相关运营工作；
- 4) 停止证书状态服务并归档相关数据；
- 5) 停止其他电子认证相关服务并归档相关数据；
- 6) 停止密码设备并归档相关密钥数据；

- 7) 及时撤销或冻结业务管理员和业务操作员的操作权限;
- 8) 对所有存档文件记录进行整理和封存;
- 9) 对所有敏感文档和数据进行安全处理和封存;
- 10) 清除主机和密码硬件设备中的敏感数据;
- 11) 其他涉及 CA 运营的数据、密钥安全的操作;
- 12) 如果有与订户电子签名认证证书签发、管理相关的外部合作机构,将在 CPS 中明确描述合作机构终止服务和通告相关的过程(暂无)。

5.9 重大事项报告

程远未来建立处理重大事件的报告流程,包括事件发生后向公司管理层、上级机构和主管部门报告的程序、时限与内容。重大事件包括但不限于:

- a) 证书认证系统迁移或改造:包括系统软件、网络、部署的重大改变。符合以下任意之一:
 - 1) 机房迁移,或机房内服务区、管理区或核心区划设范围改变;
 - 2) 变更电子签名认证证书签发逻辑;
 - 3) 新增远程证书注册子系统;
 - 4) 新增、更改或者删除用于签发电子签名认证证书的证书链;
 - 5) 其他对电子认证服务安全、用户资料安全有影响的改变。
- b) 重大安全事故:包括电子认证服务系统遭受黑客攻击、病毒入侵、数据泄露等,导致系统无法正常运行或数据安全性受到严重威胁的情形。符合以下任意之一:
 - 1) 证书签发及验证服务连续停机时间超过 24h;
 - 2) 发生根证书密钥等关键数据泄露;
 - 3) 持续或较大范围未经授权的私钥访问记录或其他异常活动;
 - 4) 系统日志持续或较大范围显示异常操作(如非授权时间或网络地址访问敏感功能)。
- c) 订户信息泄露事件:包括订户身份信息、证书申请资料等敏感数据被泄露等。符合以下任意之一:

- 1) 个人信息泄露事件影响范围较广，造成一定的经济损失或客户投诉；
- 2) 数据丢失导致无法恢复证书状态信息。
- d) 合规性事件：包括不符合相关法律法规、标准或监管要求的情形。符合以下任意之一：
 - 1) 涉及电子认证服务的司法判定；
 - 2) 收到行政部门违规通知或处罚决定。
- e) 人力资源类事件：包括一个月内核心理管理层集体离职、大规模劳动纠纷、重大职场安全事件等。符合以下任意之一：
 - 1) 涉及 2 名及以上管理层人员或 10%以上可信人员的离职；
 - 2) 劳动纠纷参与人数超过员工总数 10%，且经法院或仲裁机构生效裁决确认由 CA 承担法律责任。

5.9.1 报告的具体流程和时限

凡出现上述重大事件，均应向相应部门报告。报告的顺序为：公司管理层—工业和信息化部（后简称工信部）。

1) 证书认证系统迁移或改造事件

此类事件的报告，尤其是关于机房迁移，或机房内服务区、管理区或核心区划设范围改变和变更电子签名认证证书签发逻辑等事件，遵循“事前审批，事后汇报”的原则，公司管理层在事件发生前向工信部提交变更申请，通过后才能进行相应的变动。变动过程中程远未来将严格按照相应法律法规进行处理变更事项。程远未来将在变动完成之日起十五个工作日内向工信部报告。

2) 重大安全事故

程远未来任何岗位都有监控和报告重大安全事故的责任。一旦出现重大安全事故，应由相应负责人立即上报相应部门主管人员，部门主管人员确认事故发生后，应立即安排人员及时处理并上报公司管理层。处理人员根据程远未来相应的处理流程进行应急处理。应急处理完成后，应联系相关部门人员检查处理的结果，确认安全事故的影响范围和损失，并记录本次应急处理的过程，审批通过后存档。

程远未来管理层（包括安全策略管理委员会）在收到部门主管人员的通报后，

应实时监控事故的处理进度，并在事故处理完成后组织复盘，避免同样的事故。

程远未来将在自事件发生之日起十五个工作日内，向工信部提交相应的报告。

3) 其它事件

其它事件，包括了前文所述的订户信息泄露事件、合规性事件和人力资源类事件。程远未来将按照规定，在事件发生之日起十五个工作日内，向工信部提交相应的报告。

5.9.2 报告的内容和格式

报告的内容和格式根据工信部的最新要求进行填写。

6 认证系统技术安全控制

6.1 技术安全管理制度要求

程远未来已建立并实施相应的技术安全管理制度，制度范围覆盖密钥管理、系统开发、网络防护等领域。程远未来实施的技术安全管理制度定期接受安全策略委员会的评审，频率不低于每年一次。

6.2 密钥对的生成和安装

6.2.1 根证书密钥对的生成和安装

程远未来根证书密钥对的生成与安装要求，包括：

1) 根证书密钥生成和安装

程远未来的根证书密钥由部署在程远未来核心区内（物理隔离）的服务器密码机产生，程远未来使用的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。

RA 的签名私钥在安全控制下产生，RA 证书由程远未来签发。

2) 根证书密钥对的生成、备份、恢复、销毁过程

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（至少三人），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五选三的方式，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。

程远未来根证书密钥对进行操作时，需要事先通过安全策略委员会授权后方可进行，操作全过程进行录音录像记录。记录的保存期限为操作完成后十年。

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 5 年（参见 § 5.5.2）。归档的 CA 密钥对保存在 §6.3.1 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 §6.3.11 所述的方法进行安全地销毁。

6.2.2 订户密钥对的生成和交付

订户的密钥对可以由订户、程远未来生成。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。

订户在接收后做相应确认，确认形式不限。

订户签名密钥对的生成、交付及控制方式，符合如下三种要求之一：

1) 由订户持有的符合国家安全标准的密码模块产生和存储

订户持有的签名密钥对的产生和存储，必须遵循国家的法律政策规定，由符合国家安全标准的密码模块产生和存储。程远未来支持多种模式的签名密钥对产生方式，可以使用硬件密码模块（如：USB Key、SIM 卡等），或者使用云端可信系统的硬件密码模块，或者使用数字身份加云端可信系统的硬件密码模块，或者使用国家密码管理局批准的软件密码模块等方式，证书申请者可根据其需要进行选择。订户签名私钥不能导出密码模块且密钥长度至少为 RSA2048 位或 ECC 256 位。不管何种方式，密钥对产生的安全性都应该得到保证。

2) 由 CA 产生、保存，并提供技术措施确保订户对签名私钥的独占控制权

程远未来可根据订户或依赖方、项目特性，为订户提供密钥产生和保存服务。

程远未来在遵循国家的法律法规和相关管理制度的前提下,通过具有国家密码主管部门的相应资质的硬件密码模块产生订户公私钥对,辅以安全可靠的密钥保存系统和订户授权体系,为订户提供订户密钥对产生、保存、可信管理和使用服务,保证订户对签名私钥具有独占控制权。

订户在管理和使用密钥前,程远未来将通过包括但不限于人脸识别、随机手机短信验证码、书面授权文件等方法,验证用户身份真实性和意愿性,确保订户密钥的安全使用。

3)采用通过主管部门认可的其他创新性保护方案

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

6.2.3 加密密钥对传递给订户

订户的加密密钥由程远未来密钥管理系统生成,程远未来将通过安全途径将加密密钥对传送到最终用户手中,并确保在传送过程中不会被非授权的使用、泄露或损坏。。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。

6.2.4 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(或通过其授权的服务机构提交),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。

6.2.5 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。

6.2.6 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。

6.2.7 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。

6.2.8 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。

6.3 私钥保护和密码模块工程控制

6.3.1 CA 私钥保护和密码模块工程控制

程远未来对根证书私钥保护符合的要求,包括但不限于:

- 1) 根证书私钥保护使用通过国家密码主管部门认可的密码产品,符合 GB/T 37092-2018 第 5 章的要求

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:

- a) 接口安全:不执行规定命令以外的任何命令和操作;
 - b) 协议安全:所有命令的任意组合,不能得到私钥的明文;
 - c) 密钥安全:密钥的生成和使用必须在硬件密码设备中完成;
 - d) 物理安全:密码设备具有物理防护措施。
- 2) 根证书私钥实施严格的分割保护机制,实现单人无法获取完整私钥

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。

3) 程远未来根证书私钥备份由密钥管理员分别单独保存在有防盗措施的安全场所

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。

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 位密钥分管员中的 3 位管理员同时在场才能完成。

6.3.2 订户私钥保护和密码模块工程控制

订户与程远未来签署相关服务协议，约定签名私钥的保存方式和管理要求。签名私钥保管符合下列要求之一：

a) 订户签名私钥由订户持有

订户与程远未来签署相应的服务协议，订户须采取预防措施防止私钥及其激活数据的丢失、泄露、更改或未经授权的使用；

订户需要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。

b) 程远未来受订户委托保管订户签名私钥

1) 采用的电子签名模式

程远未来采用代理签名模式，签名方将密钥托管在程远未来，授权程远未来完成电子签名的机制。

订户签名私钥委托程远未来代为保管，程远未来依托符合安全规范的密钥管理系统统一安全存储与运维，对该密钥实施全流程安全管控。

2)采用的安全控制措施，并定期进行安全评估

程远未来在遵循国家的法律法规和相关管理制度的前提下，通过具有国家密码主管部门的相应资质的硬件密码模块产生订户公私钥对，辅以安全可靠的密钥保存系统和订户授权体系，为订户提供订户密钥对产生、保存、可信管理和使用服务，并定期进行安全评估。

3)每次签名私钥调用必须获得订户的明确授权，授权记录应完整保存

订户在管理和使用密钥前，程远未来将通过包括但不限于人脸识别、随机手机短信验证码、书面授权文件等方法，验证用户身份真实性和意愿性，确保订户密钥的安全使用。

4)向订户提供关于签名私钥及激活数据安全使用的指导与建议

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。

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。

密钥用途应与证书中的“密钥用途”（Key Usage）和“扩展密钥用途”（ExtendedKey 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。

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。

5)电子签名模式和控制措施应符合相关标准或采用经主管部门认可的其他方式。

6.3.3 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。

6.3.4 私钥归档

本处私钥归档是指订户加密证书密钥对或订户委托程远未来保管的签名私钥的归档，是将已过生命周期或暂不使用的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。

6.3.5 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。

6.3.6 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。

6.3.7 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 § 6.3.1 要求进行管理。

程远未来订户应按照 § 6.5.1 的要求，在激活私钥之前使用 PIN 码/口令或者同等强度其他方式进行确认/校验，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。

6.3.8 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。

6.3.9 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 § 6.3.4 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。

6.3.10 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。

6.4 密钥对管理的其他方面

6.4.1 公钥归档

程远未来对公钥证书进行定期归档，其最大间隔为 30 天。公钥归档是证书归档的一部分，具体要求参见 § 5.5。

6.4.2 证书操作期和密钥对使用期限

a) 签名密钥对使用期限

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。

b) 签名密钥对的使用限制

对程远未来签发的、已过期证书（包括程远未来 CA 证书和订户证书在内），其对应的签名私钥不得继续用于电子签名。

6.5 激活数据

程远未来和订户的激活数据从生成、传输、使用、保管到销毁各环节均采用足够的安全控制措施，包括但不限于：

a) 程远未来和证书订户妥善保管各自的激活数据，并采用安全的技术措施传输激活数据

程远未来 CA 私钥激活数据的生成和安装，遵循 § 6.2.1 中多人控制的要求。
程远未来 CA 私钥激活数据的保护遵循 § 6.3.1 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。订户私钥激活数据的保护遵循 § 6.3.2 的要求。

程远未来将通过安全途径将激活数据传送到最终用户手中，并确保在传送过程中不会被非授权的使用、泄露或损坏。通过网络传送时使用安全套接层协议（SSL）和其他安全协议。

b) 激活数据的安全保护

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。

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。

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。

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。

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

订户在收到硬件密码模块（如 USB Key、SIM 卡等）时，应立即使用强口令修改原有的口令。强口令由用户产生，用户产生的口令应不易猜测，还必须满足如下要求：

- 1) 口令长度至少为 8 位字符；
- 2) 至少包含一个大写字母；
- 3) 至少包含一个特殊字符和一个数字；
- 4) 不能包含多个相同或连续的字符；

6.6 计算机安全控制

程远未来已建立并实施符合 GB/T 25056-2018 中 8.2 要求的计算机安全控制体系，包括但不限于：

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：

- a) 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；
- b) 对设备定期进行检查、清洁和保养维护；
- c) 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；
- d) 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；
- e) 设备维修时，必须派有专人在场监督。

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。

程远未来对每台计算机都实行如下安全措施：

- a) 至少每半年检查一次系统升级补丁，记录系统升级审批及实施过程；
- b) 对无官方补丁支持的系统，制定网络隔离、功能限制等加强防护措施和系统更替计划；
- c) 对所有服务器和操作终端安装杀毒软件；
- d) 病毒库更新间隔为每周一次自动更新；
- e) 病毒扫描时间间隔为每周一次。

6.7 生存周期安全控制

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

6.7.1 系统开发控制

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。

6.7.2 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。

6.7.3 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。

6.8 网络的安全控制

系统网络安全的主要目的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保障系统网络安全。

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

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

6.9 时间戳

程远未来提供符合 RFC 3161 标准的时间戳服务，主要用于服务 PDF 或 OFD 版式文件的电子签章所需。程远未来时间戳服务以双机互备方式，通过 API 接口提供服务。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

程远未来签发的电子签名认证证书的格式符合 GB/T 20518 的要求，证书内容包括但不限于下列内容：

- 1) 证书版本号
符合 X.509 V3 版证书格式，版本信息存放在证书版本格式栏内。
- 2) 密码算法对象标识符

符合国家密码主管部门批准的算法对象标识符。

3) CA 和订户的名称

程远未来签发的每张公钥证书中，都包含颁发者(issuer)的信息。

数字证书中的颁发者(issuer)是 X.501 目录唯一名称，各属性的编码一般使用 UTF8String。证书的颁发者一般格式如下：C=CN, O={单位名称}, OU={部门名称}, OU={部门名称}, CN={通用名称}。

程远未来根据业务不同，使用不同的颁发者(Issuer)签发订户数字证书。程远未来共使用三个 CA 证书，因此三个对应的颁发者的具体内容如下：

a) C=CN,O= iFuture Service Co., Ltd.,O= iFuture Trust Network,CN= iFuture Enterprise CA。

b) C=CN,O= iFuture Service Co., Ltd.,O= iFuture Trust Network,CN= iFuture SignEase Subscriber CA。

c) C=CN,O= iFuture Service Co., Ltd.,O= iFuture Trust Network,CN= iFuture Certification Authority。

订户数字证书中的主体甄别名 (Subject DN) 是 X.501 目录唯一名称，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}

a) C (Country) 为 ISO 3166-1 的国家代码，如 CN 表示中国；

b) 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；

c) 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；

d) CN (Common Name) 中的内容分为以下几种：

- 个人证书中应为证书主体的姓名；
- 机构证书中应为证书主体机构的标准名称或简称；
- 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。

e) 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。

- 4) 证书策略对象标识符，其中必须包含主管部门制定的相应等级证书策略OID(见 § 1.5.1)；
- 5) 证书序列号；
- 6) 证书有效期；
- 7) 订户的电子签名验证数据；
- 8) 程远未来的电子签名；
- 9) 公钥证书的用途；
- 10) 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：

- a) 颁发机构密钥标识符 Authority Key Identifier
- b) 主体密钥标识符 Subject Key Identifier
- c) 密钥用法 Key Usage
- d) 扩展密钥用途 Extended Key Usage
- e) 私有密钥使用期 Private Key Usage Period
- f) 主体可选替换名称 Subject Alternative Name
- g) 基本限制 Basic Constraints
- h) 证书撤销列表分发点 CRL Distribution Points
- i) 私有扩展项可支持以下类型：
 - 个人身份证号码
 - 企业工商注册号
 - 企业组织机构代码
 - 企业税号
 - 统一社会信用代码

程远未来电子认证业务规则中明确了电子签名认证证书中包含证书用途、建立的流程、签名私钥的保存方式、相关的法律符合性等内容，以便于订户及依赖方了解证书内容，如对以上内容存疑，可与程远未来联系咨询。

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 GB/T 20518—2018 中 5.3 的要求，至少包括如下条目：

- 1) 版本号
- 2) 签名算法
- 3) 颁发者
- 4) 生效日期
- 5) 下次更新日期
- 6) 授权密钥标识符

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

程远未来在线证书状态服务符合 GB/T 19713-2025 中第 7 章的要求。

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 认证机构审计及相关评估

8.1 审计评估制度

程远未来制定了《程远未来审计与评估制度》。程远未来将严格按照该制度执行相应的审计评估。

- a) 程远未来审计评估的类型包括认证业务审计和全面符合性评估。
- b) 程远未来执行审计评估的频率，或是引发评估事件的条件如下：
 - 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。
- c) 程远未来每年接受主管部门的年度检查，至少每半年进行一次内部审计。

1) 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。

2) 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。内部审计人员应满足审计岗位的职责和技能要求。

3) 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。

- d) 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主题包括：

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

程远未来采用的评估方法根据评估内容确定，全面符合性评估采用法规对标、

资料审阅、现场核查、抽样测试等组合方法，以电子认证、商用密码法规及 CPS 为基准，查阅制度台账与业务档案，现场核验机房、系统、密钥管控，按比例抽验证书全流程业务，逐项比对打分，梳理合规缺陷，形成整改清单。

8.2 认证业务审计

程远未来开展的认证业务审计方式，包括但不限于：

- a) 程远未来的认证业务审计周期为每半年一次；
- b) 审计内容包括但不限于程远未来执行证书申请、续期、密钥变更、更新、撤销、冻结等业务中订户告知、身份查验、意愿记录、协议签署、资料保存的合规性；
- c) 程远未来采用抽样审计方式，审计抽样率根据依赖方的性质或项目特性，在万分之一至百分之三之间进行选择；
- d) 当审计发现问题后，由审计员通知被审计部门及时整改，及时跟踪整改落实情况。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。

8.3 全面符合性评估

程远未来开展全面符合性评估。

- a) 程远未来全面符合性评估周期为每年一次；
- b) 评估内容包括但不限于：年度电子认证服务开展情况、电子认证服务许可条件符合性情况以及认证规则和证书策略符合性情况等；
- c) 程远未来采用抽样审计方式，审计抽样率不低于 § 8.2.c 的要求；
- d) 当审计发现问题后，由审计员通知被审计部门及时整改，及时跟踪整改落实情况；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；
- e) 每年在 1 月底前将上一年度符合性评估报告报送主管部门。

8.4 评估结果的传达与发布

除非法律法规明确要求，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 证书费用

本机构开展了服务成本核算，制定了价格策略，并于程远未来官网公布各项服务收费标准，收费标准包括：

- 1) 证书颁发或更新费用；
- 2) 证书访问费用；
- 3) 撤销证书的费用；
- 4) 状态信息访问费用；
- 5) 电子签名的费用；
- 6) 签名验证的费用；
- 7) 签名验证报告的费用；
- 8) 其他服务的费用。

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

程远未来将设立不低于上一年营业收入 1.5% 的充足财力作为备用资金，以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。

备用资金的来源主要由经营回款、投资、资本注入等组成，并采用固定对公账户活定存方式进行管理。

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 非保密信息的范围

程远未来《证书策略》、《电子认证业务规则》不属于保密的信息。

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 保护保密信息的要求

各方有保护自己、其他人员和单位机密信息的要求,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 个人隐私保护

程远未来参照 GB/T 35273-2020 的规定保护个人隐私信息。

9.4.1 隐私保护方案

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 陈述和担保

9.6.1 电子认证服务机构的陈述和担保

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 服务机构的陈述和担保

程远未来授权的服务机构在参与电子认证服务过程中的承诺如下：

- 1) 提供给证书订户的服务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，不会因为服务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) 服务机构将按 CPS 的规定，及时向程远未来传输证书申请、撤销、更新等请求服务信息。

9.6.3 订户的陈述和担保

订户一旦接受程远未来签发的证书，就被视为向程远未来、服务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服务机构检查和核实；
- 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服务机构，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 依赖方的陈述和担保

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 其他参与者的陈述和担保

其他参与者的陈述与担保同 § 9.6.4。

9.7 担保免责

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。

担保免责内容包括但不限于：

- 1) 担保责任的否定描述,即明确排除程远未来不需要承担的担保责任范围，主要包含以下内容：
 - a) 排除超出法定审查义务的绝对担保责任：程远未来不对证书信息绝对真实性承担无限担保责任，仅承担合理审慎的审查义务，不担保申请人不存在任何隐瞒、伪造信息的行为，若申请人故意提交虚假、伪造的申请材料，程远未来已按照法定流程和规范要求完成核验仍无法识别的，不承担担保责任；
 - b) 排除非程远未来过错导致的交易损失担保：程远未来不对证书使用后的全部交易结果承担担保责任，仅对认证流程和证书信息的合规性负责；因订户自身未妥善保管私钥、私钥泄露、证书信息变动等未及时告知程远未来申请撤销证书或变更证书，超出证书载明使用范围使用证书，或

交易双方自身交易纠纷损失，不承担担保责任；

- c) 排除授权范围外的越权行为担保责任：通过服务机构提供服务时，程远未来仅对委托授权范围内的服务行为承担担保责任，不对服务机构超出授权范围的违规行为、越权操作承担担保责任；
- d) 排除证书失效后的后续担保责任：证书有效期届满失效后，或证书被依法撤销后，程远未来终止对该证书的认证服务，不再对失效证书继续使用产生的任何行为承担担保责任；
- e) 否定其他协议中额外明示担保责任：对于其他相关协议中超出法定要求、超出业务规则约定范围的明示担保义务，程远未来依法不承担对应担保责任。

2) 隐含担保责任是指基于法律法规的强制性要求、电子认证的行业公信力属性，无需通过合同明示约定，自动伴随电子认证服务产生的法定默示担保义务，该责任为法定责任而非意定责任，只要电子认证服务机构依法取得资质开展认证服务，就自动承担该担保责任，核心目的是保护证书依赖方基于对认证机构公信力产生的合理信赖利益；责任范围限定在法定合规义务范围内，不承担无限担保责任。

- a) 认证流程合规的隐含担保：程远未来隐含担保开展电子认证服务的全流程符合《电子签名法》《电子政务电子认证服务管理办法》以及程远未来公示的业务规则，不存在违反操作程序的违规情形，从受理申请、身份核验到证书签发、更新、撤销全环节都符合规范要求。
- b) 证书信息真实准确的隐含担保：程远未来隐含担保所签发证书中记载的核心信息，包括订户身份信息、公钥信息、证书有效期等内容，不存在明知或应知的虚假、错误、遗漏，已经尽到了合理审查核验义务。
- c) 技术安全合规的隐含担保：程远未来隐含担保自身采用的密码技术、安全存储设施、认证系统符合国家密码管理规定与技术标准，能够保障证书在有效期内不被非法篡改，保障认证过程和用户信息的安全。

3) 担保免责条款的适用规定：

- a) 申请人故意提交虚假、伪造的申请材料；
- b) 订户自身未妥善保管私钥、私钥泄露等未及时告知程远未来并申请撤销

证书；

- c) 证书信息变动等未及时告知程远未来并申请变更证书；
- d) 超出证书载明使用范围使用证书；
- e) 交易双方自身交易纠纷；
- f) 超出授权范围的违规行为、越权操作；
- g) 证书有效期届满失效后，或证书被依法撤销后，失效证书继续使用；
- h) 对其他协议中超出电子认证服务机构法定要求的担保责任。

9.8 偿付责任规则

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，程远未来及服务机构不承担责任。

9.8.1 偿付责任范围

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（技术故障、人为错误、安全漏洞等），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内承担损失或损害赔偿。

9.8.2 赔付计算方式

程远未来将依据每张证书实际收费金额的三倍进行赔付，个人证书上限不超过 200 元，机构证书和设备证书上限不超过 500 元的计算方式进行赔付。

9.8.3 赔付监督机制

程远未来建立了赔付监督机制，制定了《赔付监督管理办法》制度，按照制度以保障合理科学的执行。

9.8.4 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 § 9.16.4；
- 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 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服务机构产生损失，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。

程远未来受理赔偿业务时将内部成立赔偿案件审理小组，由订户提供赔偿申请以及相关证明材料，赔偿案件审理小组受理之日起五个工作日内将赔偿申请书和相关材料复印件提交至相关的业务部门，业务部门收到材料之日起三个工作日内向赔偿案件审理小组提供说明材料，赔偿案件审理小组根据说明材料进行调查取证等一系列工作后召开审理会议，审理会议结束后五个工作日内提出赔偿审理报告和建议，提交至技术和安全策略委员会会议审查决定，之后由安全策略委员会拟定《赔偿协议书》，报总经理代表审批签发，当《赔偿协议书》经过十五天无异议后方可转至财务部进行财务流程审批并进行支付赔偿。

9.10 有效期和终止

9.10.1 有效期

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。

9.10.2 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。

9.10.3 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。

9.11 对参与者的个别通告与沟通

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

9.12 修订和发布

9.12.1 修订程序

当本《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。

9.12.2 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。

9.12.3 必须修改业务规则的情形

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

9.13 争议处理与举证

9.13.1 争议处理

程远未来建立与证书订户、依赖方等实体在 CP/CPS、电子认证服务中产生争议的解决机制，明确了争议的受理范围、处理流程、协商时限调节规则，以及诉讼、仲裁等法定争议解决方式的管辖规则与适用条件。

程远未来受理争议的范围为仅限于证书有效期内的合法应用出现的纠纷。

处理流程为：

- 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。

争议协商时限为自争议发生之日起三十个工作日。

调解规则为：

- 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。

诉讼、仲裁等法定争议解决方式的管辖规则与适用条件为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。

9.13.2 举证

举证制度和能力体系覆盖证书全生存周期，包括但不限于：

- 1) 证书签发环节，身份验证记录、材料审查记录记录、告知记录、意愿确认记录等；

- 2) 签名环节，签名请求验证、签名操作日志、时间戳记录等；
- 3) 验证签名环节，验证请求记录、验证结果记录、异常情况处理记录等；
- 4) 提供举证材料的时间承诺为 7 个工作日内。

9.14 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》、《中华人民共和国密码法》及《电子认证服务管理办法》等。

9.15 与适用法律的符合性

无论在任何情况下，电子认证服务活动的 CA 机构、订户、依赖方等所有参与者需遵守适用的法律法规，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。在中华人民共和国境内适用的法律法规包括但不限于《中华人民共和国电子签名法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《商用密码管理条例》、《电子认证服务管理办法》、《电子认证服务密码管理办法》。

9.16 一般条款

9.16.1 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。本文档即 CPS 的全部文档，并在此声明本《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。

订户协议及依赖方协议中会标明对应的 CPS 版本。

程远未来的 CP、CPS 均以官网发布版本和内容为准。

9.16.2 分割性

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

9.16.3 强制执行

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

9.16.4 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。

9.17 其他条款

无规定。