重庆程远未来电子商务服务有限公司

电子政务电子认证服务业务规则

E-Gov Certification Practice Statement

Version 1.2

生效日期： 2024年04月11日

重庆程远未来电子商务服务有限公司

电子政务电子认证服务业务规则

程远未来版权声明

【文档信息】 公开

文档名称	重庆程远未来电子政务电子认证服务业务规则		
文档编号	CYWL-II02-2019		
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 起草小组	**制作日期**	2024.04.09
复审人	安全策略委员会	**复审日期**	2024.04.10
批准人	安全策略委员会	**批准日期**	2024.04.11
发布人	安全策略委员会	**发布日期**	2024.04.11
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
2018 年 12 月	V1.0	创建	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
2019 年 3 月	V1.1	修改与 GM/Z 4001《密码术语》不一致及部分未描述具体落实措施等	刘玉祥、魏薇	安全策略委员会	安全策略委员会
2024 年 4 月	V1.2	修改补充 CRL 备份保存时间及更新投诉电话、邮箱等信息	李海波、蔡伟	安全策略委员会	安全策略委员会

目　　录

目　　录 4
第一章 概括性描述 1
1.1 概述 1
1.1.1 公司简介 1
1.1.2 电子政务电子认证服务业务规则 1
1.2 文档名称与标识 1
1.3 电子认证活动参与者 1
1.3.1 电子认证服务机构 1
1.3.2 注册机构 2
1.3.3 证书持有者 2
1.3.4 证书依赖方 2
1.3.5 其他参与者 2
1.4 证书应用 2
1.4.1 适合的证书应用 2
1.4.2 限制的证书应用 3
第二章 规则依据文件 3
第三章 术语和定义 3
第四章 符号和缩略语 4
第五章 管理规范 4
5.1 策略文档管理机构 4
5.2 联系方式 4
5.3 CPS 批准程序 5
第六章 电子政务电子认证服务业务内容及相关要求 6
6.1 数字证书服务 6
6.1.1 服务内容 6
6.1.2 数字证书类型 6
6.1.3 身份标识与鉴别 6
6.1.4 数字证书服务操作要求 10
6.2 应用集成支持服务 21
6.2.1 证书应用接口程序 21
6.2.2 证书应用方案支持 21
6.2.3 证书应用接口集成 21
6.3 信息服务 22

6.3.1 服务内容 22
6.3.2 服务管理规则 22
6.3.3 服务方式 23
6.4 使用支持服务 23
6.4.1 服务内容 23
6.4.2 服务能力 24
6.4.3 服务质量 25
6.5 安全保障 25
6.5.1 认证机构设施、管理和操作控制 25
6.5.2 认证系统技术安全控制 33
第七章 电子政务电子认证服务操作规范 37
7.1 数字证书服务操作规范 37
7.1.1 数字证书格式 37
7.1.2 身份标识与鉴别 37
7.1.3 数字证书服务操作要求 38
7.2 应用集成支持服务操作规范 44
7.2.1 服务策略和流程 44
7.2.2 应用接口 44
7.2.3 集成内容 45
7.3 信息服务规范 45
7.3.1 服务内容 45
7.3.2 服务管理规则 46
7.3.3 服务方式 46
7.4 使用支持服务操作规范 47
7.4.1 服务内容 47
7.4.2 服务方式 48
7.4.3 服务质量 48
7.5 安全保障规范 48
7.5.1 认证机构设施、管理和操作控制 49
7.5.2 认证系统技术安全控制 62
第八章 法律责任相关要求 68
8.1 要求 68
8.2 内容 68
8.2.1 费用 68
8.2.2 财务责任 69

8.2.3 业务信息保密 70
8.2.4 个人隐私保密 70
8.2.5 知识产权 71
8.2.6 陈述与担保 72
8.2.7 担保免责 73
8.2.8 有限责任 73
8.2.9 赔偿 73
8.2.10 有效期限与终止 74
8.2.11 对参与者的个别通告与沟通 75
8.2.12 修订 75
8.2.13 争议处理 75
8.2.14 管辖法律 76
8.2.15 与适用法律的符合性 76
8.2.16 一般条款 76
8.2.17 其他条款 76

第一章 概括性描述

1.1 概述

1.1.1 公司简介

重庆程远未来电子商务服务有限公司（以下简称“程远未来”）成立于2014年12月，具备国家密码管理局颁发的电子认证服务使用密码许可证（证书编号:0047）和工业和信息化部颁发的电子认证服务许可证（许可证编号:ECP50011218047）。程远未来致力于为电子政务、电子商务及社会信息化等应用提供优质的电子认证服务。

1.1.2 电子政务电子认证服务业务规则

《重庆程远未来电子商务服务有限公司电子政务电子认证服务业务规则》（简称E-Gov CPS，本CPS）根据国家相关法律法规的要求,详细阐述了程远未来CA提供的电子政务电子认证业务所遵循的规范、电子政务电子认证服务整个过程以及电子认证服务各方所承担的责任范围等。

本规范适用于程远未来及其分支机构，并通过公开发布的渠道告知电子签名证书持有者、依赖方等相关参与者，以确保程远未来所提供的电子认证服务是权威、安全、可靠的规范化第三方服务。对于程远未来所提供的认证服务过程的责任范围，本业务规则也给予了明确的规定。

1.2 文档名称与标识

本文档名称为《重庆程远未来电子商务服务有限公司电子政务电子认证服务业务规则》，是程远未来对所提供的电子政务电子认证及相关业务的全面描述，对象标识符E-Gov CPS为“E-Gov Certificate Practice Statement”的缩写。本文档中，E-Gov CPS等同于本节中定义的文档名称和适用名称。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

电子认证服务机构是受用户信任、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。程远未来通过为从事电子交易活动的各方主体颁发数字证书、提供证书验证服务等手段而成为

电子认证活动的参与主体。

1.3.2 注册机构

程远未来的数字证书电子政务注册机构（下文简称注册机构）是经程远未来正式授权后的业务分支机构，包括证书注册审核(RA)中心、证书本地受理(LRA) 点等。注册机构是为程远未来的证书申请者建立注册过程的实体。

注册机构可以由程远未来自建或授权的第三方机构建立。当注册机构由第三方机构建立时，程远未来必须与其签订协议，明确双方的权利和义务。

1.3.3 证书持有者

证书持有者是拥有电子认证服务机构签发的有效证书的实体，可以是个人、机构或基础设施的组成部件如路由器、防火墙、服务器或用于安全通信的其他设备。

1.3.4 证书依赖方

证书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证书持有者，也可以不是证书持有者。

1.3.5 其他参与者

指为程远未来的电子认证活动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，程远未来颁发的证书可以广泛应用在电子政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时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：

个人证书：包括各级政务部门的工作人员和参与电子政务业务的社会公众个人颁发的证书，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，包括网上报税等，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。

机构证书：包括政务机关和参与电子政务业务的企事业单位，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，包括参加政府招投标业务，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。

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 限制的证书应用

证书禁止在任何违反国家法律、法规或破坏国家安全的情形下使用。否则，由此造成的法律后果由证书持有者自己承担。

程远未来签发的数字证书禁止的应用范围包括：

1）国家法律法规所规定的不允许使用的范围；

2）破坏国家安全、环境安全和人身安全的危险环境；

3）程远未来与证书持有者约定的证书禁止应用的范围。

第二章 规则依据文件

本 CPS 以下列文件为依据：

《中华人民共和国电子签名法》	中华人民共和国主席令（第十八号）	2004 年
《电子政务电子认证服务管理办法》	国家密码管理局	2009 年
《电子认证服务密码管理办法》	国家密码管理局	2009 年
《电子政务电子认证服业务规则规范》	国家密码管理局	2010 年
《电子政务电子认证基础设施建设要求》	国家密码管理局	2010 年
《电子政务电子认证服务质量评估要求》	国家密码管理局	2010 年
《信息安全技术 证书认证系统密码及其相关安全技术规范》	国家标准	2010 年
《基于 SM2 密码算法的数字证书格式规范》	国家密码管理局	2012 年
《证书应用综合服务接口规范》	国家密码管理局	2012 年

第三章 术语和定义

项目	概念定义
证书认证机构	对数字证书进行全生命周期管理的实体。也称为电子认证服务机构。
注册机构	受理数字证书的申请、更新、恢复和注销等业务的实体。
数字证书	也称公钥证书，由证书认证机构（CA）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。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。
数字签名	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。

密码模块	实现密码运算功能的、相对独立的软件、硬件固件或其组合。
密钥	控制密码算法运算的关键信息或参数。
私钥	非对称密码算法中只能由拥有者使用的不公开密钥。
公钥	非对称密码算法中可以公开的密钥。
公钥基础设施	基于公钥密码技术实施的具有普适性的基础设施，可用于提供机密性、完整性、真实性及抗抵赖性等安全服务。

第四章 符号和缩略语

项目	缩写定义(英文)	缩写定义(中文)
CA	Certification Authority	证书认证机构
KMC	Key Management Center	密钥管理中心
RA	Registration Authority	注册机构
CRL	Certificate Revocation List	证书撤销列表
MAC	Message Authentication Code	消息鉴别码
ECC	Elliptic Curve Crypto graphyalgorithm	椭圆曲线密码算法
FAQ	Frequently Asked Questions	经常问到的问题
PKI	Public Key Infrastructure	公钥基础设施
USB KEY	Universal Serial Bus Key	采用 USB 接口的证书存储介质
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议

第五章 管理规范

程远未来安全策略委员会是程远未来电子认证服务所有策略的最高管理机构，负责审核批准CPS，并作为CPS实施检查监督的最高决定机构。

5.1 策略文档管理机构

程远未来成立安全策略委员会，作为本机构电子政务电子认证服务业务规则的管理机构，对电子政务电子认证服务业务规则进行维护与管理，包括：

1)确定本CPS的维护职责，并建立合理、有效的修订和批准流程；

2)定期对存在的业务风险进行评估，并及时对本CPS进行修订；

3)按照《电子政务电子认证服务管理办法》规定，将修订后的本CPS及时报国家密码管理局备案，并在服务范围公开发布。

程远未来安全策略委员会由来自于公司管理层、综合管理中心、营销中心、产品研发中心、运营中心等拥有决策权的合适代表组成。

5.2 联系方式

程远未来公布以下对外的相关联系方式，任何有关本 CPS 的问题、建议、疑

问等，均可按照下述方式联系程远未来:

1)本 CPS 的发布地址： http://www.ifutureca.com

2)网站地址：http://www.ifutureca.com/

3)电子邮箱：weiwei68@creditease.cn

4)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）

5)联系部门：客服部

6)电话号码：023-63063149

7)传真号码：023-63061694

5.3 CPS 批准程序

程远未来按照以下方式处理本 CPS 的起草制定、审批、发布、变更、备案等流程：

1）起草小组成立和 CPS 指定

程远未来安全策略委员会召集会议，指定相关部门和人员成立起草小组。CPS 起草小组根据《电子政务电子认证服务业务规则规范》编写 CPS，在编写过程中应及时向程远未来安全策略委员会汇报制定进展，并就有关问题召集相关人员讨论。

2）审批

本 CPS 由起草小组编写制定后，提交程远未来安全策略委员会审核。程远未来安全策略委员会议一致通过后，即作为正式版本。

3）发布

根据服务范围和服务对象要求，程远未来采取如下的方式发布本 CPS：

（1）以电子的方式，在公司的官方网站发布。

（2）以书面的方式，客户服务部门可以根据需求提供。

4）变更

根据国家的政策法规、技术要求、标准的变化及业务发展情况等需要对本CPS进行修订，由起草小组编写修改建议报告，提交程远未来安全策略委员会审核。经过批准通过后，按照前述方式进行对外发布。

5）备案

根据《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法》的规定，程远未来安全策略委员会在批准本CPS的制定或修订后，程远未来将及时向国家密码管理局备案。

第六章 电子政务电子认证服务业务内容及相关要求

程远未来电子政务电子认证服务严格按照《电子政务电子认证服务管理办法》所规定的服务内容及要求开展。

6.1 数字证书服务

6.1.1 服务内容

程远未来面向电子政务活动中的政务部门和企事业单位、社会团体、社会公众等电子政务用户提供证书申请、证书签发、证书更新、证书撤销以及密钥生成、备份和恢复等服务。

6.1.2 数字证书类型

程远未来提供以下类型的数字证书：

1.个人证书：为各级政务部门的工作人员和参与电子政务业务的社会公众颁发的证书，用以代表个体的身份，如：某局局长、某局职员或参加纳税申报的个人等。

2.机构证书：用以代表政务机关和参与电子政务业务的企事业单位的身份，如：某部委、某局或参加政府招投标业务的投标企业等。

3.设备证书：为电子政务系统中的服务器或设备颁发的数字证书，用以代表服务器或设备身份的真实性，如：服务器身份证书、SSL 服务器证书、IPSec VPN 设备证书等。

4.其他类型证书：为满足电子政务相关应用的特殊需求而提供的其他应用类型的证书，如：代码签名证书等。

以上各类数字证书格式符合《电子政务数字证书格式规范》的要求，在标识实体名称时，保证了实体身份的唯一性，且名称类型支持国家相关密码规范的标准协议格式。

6.1.3 身份标识与鉴别

6.1.3.1 命名

程远未来严格按照《电子政务数字证书格式规范》的要求为电子政务数字证书

命名。

6.1.3.1.1 名称类型

程远未来颁发的数字证书，根据证书对应实体的类型不同，其实体名字可以是人员姓名、组织机构名称、部门名、域名等，证书包含证书持有者和颁发机构主题甄别名，对证书申请者的身份和其他属性进行鉴别，并以不同的标识记录其信息。证书持有者的标识命名，以甄别名形式包含在证书主体内，是证书持有者的唯一识别名。

程远未来的证书符合 X.509 标准，分配给证书持有者实体的甄别名，采用X.500标准命名方式，格式如下：

属性	值	示例
Email=	邮件地址	cywl@126.com
Common Name （CN） =	通用名	iFutureCA
Locality （L） =	市/盟	重庆
State or Province （S） =	省/自治区	重庆
Organizational Unit （OU） =	组织机构	运营部
Organization（O） =	组织	程远未来
Country（C） =	国家	CN

程远未来的证书包含颁发者的甄别名称，格式如下：

属性	值	示例
Common Name （CN） =	通用名	iFutureCA
Country（C） =	国家	CN

6.1.3.1.2 对名称意义化的要求

程远未来签发的个人实体证书、组织机构通用数字证书、服务器证书等包含的命名应具有通常理解的语义，用它可以确定证书主题中的个人、机构或设备的身份。对于具有特殊要求的应用中，程远未来可以按照一定的规则为证书持有者指定特殊的名称，并且能够把该类特殊的名称与一个确定的实体（个人、单位或设备）唯一联系起来。

6.1.3.1.3 证书持有者的匿名或伪名

本 CPS 规定，程远未来的证书持有者在进行数字证书申请时不能够使用匿名或伪名。

6.1.3.1.4 理解不同名称的形式的规则

程远未来签发的数字证书格式符合《基于 SM2 密码算法的数字证书格式规范》标准，甄别名的命名规则由程远未来定义。

6.1.3.1.5 名称的唯一性

在程远未来信任域内，不同证书持有者证书的主题甄别名不能相同，必须是唯一的。但对于同一证书持有者，可以用其主体名为其签发多张证书，但证书的密钥用法扩展项不同。当证书申请中出现不同证书持有者存在相同名称时，遵循先申请者优先使用，后申请者增加附加识别信息予以区别的原则。

6.1.3.2 证书申请人的身份确认

6.1.3.2.1 证明持有私钥的方法

程远未来通过以下两个条件来证明证书持有者对私钥的持有：

1）通过证书请求中所包含的数字签名来证明证书持有者持有与注册公钥对应的私钥。

a）证书持有者在客户端生成签名密钥的公私钥对；

b) 证书持有者使用私钥对证书请求信息签名，并连同公钥一同提交 CA 系统；

c) CA 使用证书持有者公钥验证证书持有者签名。

2) 证书持有者必须妥善保管自己的私钥。

6.1.3.2.2 组织机构身份的鉴别

程远未来在把证书签发给组织机构、组织机构拥有的设备或组织机构的代表人时，对组织机构的身份鉴别包含如下两方面内容：

1) 确认组织机构是确实存在的、合法的实体。

2) 确认该组织机构知晓并授权证书申请，代表组织机构提交证书申请的人是经过授权的。

组织机构申请者填写数字证书申请表（一式二份），经过单位授权代表的签署及单位盖章，表示接受证书申请的有关条款，并承担相应的责任。程远未来注册机构必须对证书持有者进行以下资料的鉴别：

1）申请机构组织机构代码证的复印件；

2）申请机构的营业执照副本复印件，如果没有营业执照，则提供书面申请表上可选的其他有效证件的副本复印件。部分有效证件如下：

- 营业执照

- 企业法人营业执照
- 事业单位法人登记证
- 税务登记证
- 社会团体法人登记证
- 政府批文
- 其他有效证件

3）经办人身份证原件与复印件。

6.1.3.2.3 个人身份的鉴别

程远未来在把证书签发给个人时，须对证书持有者进行身份鉴别。对个人身份鉴别包含以下两方面内容：

1）确认个人的身份是确实存在的、合法的实体。

2）委托他人申请的，需要出示授权文书，确认证书持有者知晓并授权证书申请，代表他人提交证书申请的人是经过授权的，并对授权代表进行同等方式个人身份鉴别。

3）把证书签发给政府部门个人时，还应进行以下鉴证工作：申请人提交由所属政府部门签章的证明文件，明确组织、部门与证书中所列的名称一致，并证明申请人属于该部门。

6.1.3.2.4 不进行验证的证书持有者信息

通常，除了该类型证书所必须要求的身份信息需要得到明确、可靠的验证以外，证书其他任何不被要求验证的信息可以在申请时不被要求验证。

对于没有验证的证书持有者信息，程远未来不承诺相关信息的真实性，不承担相关的法律责任。

6.1.3.2.5 授权确认

除自然人申请个人证书外的用户可授权经办人来办理数字证书业务，但需要在相关业务表格上加盖单位有效公章或提供授权文件，作为机构对经办人的授权确认。

6.1.3.2.6 互操作准则

对于程远未来以外的国家认可的其他证书服务机构，且与程远未来签署了相应的协议，可以与程远未来进行互操作，程远未来将依据协议的内容，接受非程远未来的发证机构鉴别过的信息，并为之签发相应的证书。

如果国家法律法规对此有规定，程远未来将严格予以执行。

6.1.3.3 密钥更新请求的标识与鉴别

6.1.3.3.1 常规密钥更新的标识与鉴别

对于常规密钥更新，证书持有者应提交能够识别原证书的足够信息，并使用更新前的私钥对包含新公钥的申请信息签名。对申请的鉴别应满足以下条件：

1) 申请对应的原证书存在并且由程远未来签发；

2) 用原证书上的证书持有者公钥对申请的签名进行验证；

3) 基于原注册信息进行身份鉴别。

证书持有者也可以选择一般的初始证书申请流程，按照初始身份验证步骤进行常规密钥更新，按照要求提交相应的证书申请和身份证明资料。

程远未来注册机构的审核人员合理、审慎地核对申请资料的原件与复印件，根据审核人员的管理规定对申请者的资料的真实性进行审查，并进行批准或拒绝的操作。

密钥更新会造成使用原密钥对加密的文件或数据无法解密，因此，证书持有者在申请密钥更新前，必须确认使用原密钥对加密的文件或数据已经解密，否则，由此造成的损失，程远未来将不承担责任。

6.1.3.3.2 撤销后密钥更新的标识与鉴别

程远未来不提供证书被撤销后的密钥更新。证书持有者必须重新进行身份鉴别，按照初始身份验证步骤向程远未来申请重新签发证书。

6.1.3.4 撤销请求的标识与鉴别

在程远未来的证书业务中，证书撤销请求可以来自证书持有者，也可以来自程远未来。当程远未来注册机构有充分的理由撤销证书持有者时，有权依法撤销证书，这种情况无须进行鉴证。如果证书持有者主动要求撤销证书，则需要递交初始身份验证时的申请材料，程远未来对申请人进行身份鉴别，确认要撤销证书的人或组织确实是证书持有人本人或被授权人。如果由于条件的限制无法进行现场审核时，程远未来可以通过电话、传真、邮政信函或其他第三方证明等合理方式对申请者的身份予以鉴别验证。如果是司法机关依法提出撤销，程远未来将直接以司法机关提供的书面撤销请求文件作为鉴别依据，不再进行其他方式的鉴别。

6.1.4 数字证书服务操作要求

6.1.4.1 证书申请

6.1.4.1.1 信息告知

程远未来在本 CPS 中阐述了受理证书申请的所有流程及要求，并通过网站、现场咨询、热线电话、电子邮件等方式告知证书申请者及证书持有者所必须提交的材料和办理流程。

对于个人证书，申请者到程远未来受理点填写或到程远未来网站下载填写《个人数字证书业务申请表》，并提供个人身份证明文件及其复印件一份，例如：身份证、军官证、护照、警官证、士兵证、士官证、文职干部证、及其他法律法规和政府政策认可的证明文件等。

政府、机构部门中的个人申请证书时，还需提交个人所在单位许可授权证明（申请表加盖单位公章）及单位证明文件；如果是委托申请的，还需提供经办人被授权证明，证明代表他人提交证书申请的人是经过单位授权的。

对于机构证书，申请者填写《机构数字证书业务申请表》，并提供单位对经办人的授权委托证明，单位的企业法人营业执照、事业单位法人登记证、税务登记证、组织机构代码证、社会团体法人登记证、政府批文及其他有效证件，经办人的身份证和程远未来可能需要的其他文件。

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。

组织机构申请机构证书时，由机构授权人员申请。

设备证书由域名或设备拥有机构，或获得域名或设备使用授权的机构中的授权人申请。

6.1.4.1.2 申请的提交

证书申请由证书持有者或相应的授权人提交。

非证书持有者代表组织机构进行批量证书申请的还须获得该组织的授权。

程远未来提供现场、邮寄等多种方式的证书受理申请。

6.1.4.1.3 注册过程与责任

1. 证书的注册过程

证书持有者填写相应的证书申请表单。

证书持有者携带相应的证明材料到程远未来的注册机构（RA 或 LRA）进行证书申请，注册机构审核通过后，录入申请资料。其中审核员和信息录入员分别为两

个不同的系统操作人员。

注册机构向程远未来提交证书请求，通过应用安全协议发送至程远未来。

程远未来在处理每一个证书申请中，满足以下条件：

1) 保留对最终实体身份的证明和确认信息。
2) 保证证书申请者和持有者信息不被篡改、私密信息不被泄漏。
3) 注册过程保证所有证书申请者明确同意相关的证书申请者协议。
4) 按本CPS的规定产生一个密钥对，并将公钥通过网络安全传输协议传给程远未来或其注册机构。

2. 责任

证书持有者有责任向程远未来提供真实、完整和准确的证书申请信息和资料。

注册机构承担对证书持有者提供的证书申请信息与身份证明资料的一致性检查工作，同时承担相应审核责任。

注册机构对申请材料有保密的责任。

6.1.4.2 证书申请处理

6.1.4.2.1 执行识别与鉴别功能

当程远未来及其注册机构接受到证书持有者的证书申请后，应按本CPS 6.1.3.2.2、6.1.3.2.3、6.1.3.2.4及 6.1.3.2.5的要求，对证书持有者进行身份识别与鉴别。

程远未来在处理证书申请过程中，将通过有效手段确保证书信息与正确的申请信息相符，并将证书签发给正确的申请者。

6.1.4.2.2 证书申请批准和拒绝

依据识别与鉴别的信息，程远未来注册机构有权决定接受或拒绝证书持有者的申请。

如果符合下述条件，程远未来注册机构接受证书持有者的证书申请，为证书申请者办理证书签发服务：

1）成功标识和鉴别了证书持有者的身份信息；

2）证书持有者接受证书持有者协议的内容和要求；

3）证书持有者按照规定支付了相应的费用，另有协议规定的情况除外。

如果发生下列情形之一，程远未来注册机构有权拒绝证书持有者的证书申请，并在 24 小时内通过现场或者电话、邮件等方式告知拒绝原因：

1）该申请未完成标识和鉴别的过程；

2）证书持有者不能提供所需要的补充文件；

3）证书持有者不接受或者反对证书持有者协议的内容和要求；

4）没有或者不能够按照规定支付相应的费用；

5）程远未来注册机构认为批准该申请将会对程远未来带来争议、法律纠纷或者损失。

6.1.4.2.3 处理证书申请的时间

程远未来及注册机构将在合理时间内完成证书请求处理。在申请者提交资料齐全且符合要求的情况下，处理证书请求的最长响应时间不超过48小时。

6.1.4.3 证书签发

6.1.4.3.1 证书签发中 RA 和 CA 的行为

在证书的签发过程中RA的管理员负责证书申请的审批，并通过操作RA系统将签发证书的请求发往CA的证书签发系统。RA 发往CA的证书签发请求信息须有RA的身份鉴别与信息保密措施，并确保请求正确发送至CA证书签发系统。

CA 的证书签发系统在获得RA的证书签发请求后，对来自RA的信息进行鉴别与解密，对于有效的证书签发请求，证书签发系统签发证书持有者证书。

程远未来在批准证书申请之后，将签发证书。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

通常程远未来签发的证书在24小时内生效。

6.1.4.3.2 CA 和 RA 通知证书申请者证书的签发

如果证书申请获得批准并签发，RA 将通过多种方式告诉证书申请者如何获取证书。

程远未来对证书申请者的通告提供以下几种方式：

1) 电子或纸质的受理回执；

2) 电子邮件（e-mail）；

3) 通过面对面的方式，通知证书持有者（如申请者到受理点领取等方式）；

4) 其他程远未来认为安全可行的方式。

6.1.4.4 证书接受

6.1.4.4.1 构成接受证书的行为

在程远未来数字证书签发完成后，程远未来将把数字证书当面或寄送给证书持有者，证书持有者从获得证书起就被视为已同意接受证书。证书持有者接受数字证

书后，应妥善保存其证书对应的私钥。

6.1.4.4.2 电子认证服务机构对证书的发布

对于证书申请者明确表示拒绝发布证书信息的，程远未来不发布该证书申请者证书信息。没有明确表示拒绝的，程远未来将证书信息发布到目录系统。

程远未来采用主、从目录服务器结构来分布所签发证书。签发完成的数据直接发布到主目录服务器中，然后通过主从映射，将主目录服务器的数据自动同步到从目录服务器中，供证书持有者和依赖方查询和下载。

6.1.4.4.3 电子认证服务机构对其他实体的通告

程远未来不具有向其他实体进行单独通告的义务，但使用证书的各类实体可以通过程远未来查询服务获得所需证书信息。

6.1.4.5 密钥对和证书的使用

程远未来要求证书持有者密钥对和证书的使用不能超过其规定使用范围，否则程远未来不承担由证书持有者违规使用而造成的任何责任。

6.1.4.5.1 证书持有者私钥和证书的使用

证书持有者接受到数字证书后，应妥善保存其证书对应的私钥。证书持有者可以从程远未来证书目录服务器中下载个人或其他数字证书。

对于签名证书，其私钥仅用于对信息的签名。在可能的情况下，签名证书应同被签名信息一起提交给依赖方。证书持有者使用私钥对信息签名时，应该确认被签名的内容。对于加密证书，其私钥可用于对采用对应公钥加密的信息解密。在证书到期或被撤销之后，证书持有者必须停止使用该证书对应的私钥。

6.1.4.5.2 依赖方公钥和证书的使用

依赖方只能在接受程远未来协议要求的前提下，才能依赖程远未来证书持有者证书。在信任证书和签名前，依赖方必须根据环境和条件进行合理地判断并做出决定。

在依赖证书前，依赖方必须独立的进行如下评估和判断：

1）证书是否由可信任的CA所签发；

2）证书被适当的使用，判断该证书没有被用于电子政务电子认证服务业务规则或者法律法规禁止或限制的使用范围；

3）证书的使用与证书密钥用途包含内容是否一致；

4）查询证书及其证书信任链中的证书状态，如果证书持有者证书或其信任链内

的任何证书已经被撤销，依赖方必须独立去了解该证书对应的私钥所做的签名是否是在撤销之前做的，是否可以依赖，并独立承担相应的风险。

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

获得对方的证书和公钥，可以通过查看证书以了解对方的身份，通过公钥验证对方电子签名的真实性。

6.1.4.6 证书更新

证书更新指在仅延长证书持有者的证书有效期情况下，为证书持有者签发一张新证书。证书更新时无需再提交证书注册信息，证书持有者仅需提交能够识别原证书的足够信息，如证书持有者甄别名、证书序列号等，使用原证书的私钥对包含公钥的更新申请信息签名。

6.1.4.6.1 证书更新的情形

为保证证书及其密钥对的安全有效和证书持有者的权利，程远未来会为签发的证书设置有效期。证书持有者必须在证书有效期到期前3个月内，到程远未来注册机构申请更新证书。

6.1.4.6.2 请求证书更新的实体

请求更新的实体为证书持有者本人或其授权代表。

6.1.4.6.3 处理证书更新请求

对于证书更新，其处理过程包括申请验证、鉴别、签发证书。对申请的验证和鉴别须基于以下几个方面：

1) 证书持有者的原证书存在并且由程远未来所签发；

2) 用原证书上的证书持有者公钥对申请的签名进行验证；

3) 基于原注册信息安装证书更新时的要求进行身份鉴别。

在以上验证和鉴别通过后程远未来才可批准签发证书。

证书持有者也可以选择一般的初始证书申请流程进行证书更新，按照本CPS的要求提交相应的证书申请和身份证明资料。程远未来在任何情况下都可将这种初始证书申请的鉴别方式作为证书更新时的鉴别处理手段。

6.1.4.6.4 颁发新证书时对证书持有者的通告

同第6.1. 4.3.2 节“证书持有者证书签发的通知”。

6.1.4.6.5 构成接受更新证书的行为

同第 6.1.4.4.1 节“构成接受证书的行为”。

6.1.4.6.6 电子认证服务机构对更新证书的发布

同第 6.1.4.4.2 节“电子认证服务机构对证书的发布”。

6.1.4.6.7 电子认证服务机构对其他实体的通告

同第 6.1.4.4.3 节“电子认证服务机构对其他实体的通告”。

6.1.4.7 证书密钥更新

证书密钥更新是指不改变证书中包含的信息的情况下，产生新的密钥对，并由程远未来签发新证书。

6.1.4.7.1 证书密钥更新的情形

证书证书持有者申请更换密钥的情形主要有：

1) 证书的密钥泄露。对此，证书持有者负有立即告知程远未来的责任；

2) 证书到期时，要求更换证书密钥；

3) 证书丢失；

4) 其他。

例如，由于信息技术的不断更新，为了保证证书的安全性，程远未来有权要求证书持有者更换证书的密钥。

6.1.4.7.2 请求证书密钥更新的实体

请求密钥更新的实体为证书持有者本人或其授权代表。

6.1.4.7.3 证书密钥更新请求的处理

同第 6.1.4.6.3 节“证书更新请求的处理”。

6.1.4.7.4 证书持有者新证书签发的通知

同第 6.1.4.6.4 节“通知证书持有者新证书签发”。

6.1.4.7.5 构成接受密钥更新证书的行为

同第 6.1.4.4.1 节“构成接受证书的行为”。

6.1.4.7.6 电子认证服务机构对密钥更新证书的发布

同第 6.1.4.4.2 节“电子认证服务机构对证书的发布”。

6.1.4.7.7 电子认证服务机构对其他实体的通告

同第 6.1.4.4.3 节“电子认证服务机构对其他实体的通告”。

6.1.4.8 证书撤销

6.1.4.8.1 证书撤销的条件

程远未来、注册机构及证书持有者在发生下列情形之一时，申请撤销数字证书：

A. 政务机构的证书持有者工作性质发生变化；

B. 政务机构的证书持有者受到国家法律法规制裁；

C. 证书持有者提供的信息不真实；

D. 证书持有者没有或无法履行有关规定和义务；

E. 程远未来、注册机构或最终证书持有者有理由相信或强烈的怀疑一个证书持有者的私钥安全已经受到损害；

F. 政务机构有理由相信或强烈怀疑其下属雇员的私钥安全已经受到损害；

G. 和证书持有者达成的证书持有者协议已经终止；

H. 证书持有者请求撤销其证书；

I. 证书仅用于依赖方主导的系统并由依赖方提出撤销申请的；

J. 法律、行政法规规定的其他情形。

6.1.4.8.2 证书撤销的发起

以下实体可以请求撤销证书持有者证书：

A. 批准证书持有者证书申请的程远未来、注册机构、电子政务机构或依赖方在满足证书撤销条件的前提下，可以要求撤销证书持有者证书；

B. 对于个人证书，证书持有者可以请求撤销他们自己的个人证书；

C. 对于机构证书，只有机构授权的代表有资格请求撤销已经签发给该机构的证书；

D. 对于设备证书，只有拥有该设备的机构授权的代表有资格请求撤销已经签发给该设备的证书；

E. 司法机关等公共权力部门的授权代表可以要求撤销证书持有者证书。

6.1.4.8.3 证书撤销的处理

证书持有者到程远未来注册机构书面填写《程远未来数字证书申请表》，并注明撤销的原因。程远未来注册机构按照第 6.1.3 节“身份标识与鉴别”对证书持有者提交的证书撤销申请进行审核。

如是强制撤销，程远未来注册机构管理员可以对证书持有者证书进行强制撤销，撤销后立即通知该证书证书持有者。强制撤销的命令来自于：程远未来、程远未来注册机构或司法机关等公共权力部门。

撤销后的证书在 24 小时内发布 CRL 或被直接签发 CRL，向外界公布。

证书撤销后，通过当面、电子邮件、电话、传真等方式告知用户或依赖方证书撤销结果。

6.1.4.8.4 撤销请求宽限期

当最终证书持有者发现出现第6.1.4.8.1章节中的情况时，应该尽快提出证书撤销请求，撤销请求必须在发现密钥泄密后或有泄密嫌疑8小时以内提出，其它撤销原因从发现需要撤销证书到向程远未来或注册机构提出撤销请求的时间间隔必须在24小时以内提出。

6.1.4.8.5 电子认证服务机构处理撤销请求的时限

程远未来从收到证书撤销请求起24小时内完成请求的处理。

6.1.4.8.6 依赖方检查证书撤销的要求

依赖方在信任证书前，必须对证书的状态进行检查，包括：

1）在使用证书前根据程远未来最新公布的CRL检查证书的状态；

2）验证CRL的可靠性和完整性，确保它是经程远未来发行并电子签名的。

依赖方应根据程远未来公布的最新CRL或提供的OCSP服务确认使用的证书是否被撤销。如果公布证书已经撤销，而依赖方没有检查，由此造成的损失由依赖方承担。

6.1.4.8.7 CRL 发布频率

程远未来CRL发布周期为 24 小时，特殊紧急情况下可以立即签发CRL。

6.1.4.8.8 CRL 发布的最大滞后时间

程远未来撤销的证书从被撤销到被发布到CRL上的滞后时间最大为24小时。

6.1.4.8.9 在线状态查询的可用性

程远未来向证书持有者提供7×24小时在线证书状态查询服务（OCSP）。

6.1.4.8.10 在线状态查询要求

依赖方在信赖一个证书前必须通过证书状态查询检查该证书的状态。如果依赖方不希望通过最新的相关证书撤销列表来检查证书状态，则应通过可用的OCSP服务

对证书状态进行在线检查。

6.1.4.8.11 撤销信息的其他发布形式

程远未来网站（http://www.ifutureca.com）提供CRL文件下载。

6.1.4.8.12 密钥损害的特别要求

程远未来所有证书持有者在发现证书密钥受到损害时，应立即通知程远未来撤销证书。

6.1.4.9 证书状态服务

程远未来通过CRL、OCSP、LDAP提供证书状态服务。

6.1.4.9.1 操作特征

程远未来提供以下三种方式为证书证书持有者提供证书状态查询：

1）通过发布服务器采用http方式发布CRL，其可信度及安全性由CA证书的签名来保证。证书持有者需要将CRL下载到本地后进行验证，包括CRL的合法性验证和检查 CRL中是否包含待检验证书的序列号；

2）提供OCSP（在线证书状态查询）服务，以网络服务的方式提供证书状态信息，符合RFC2560标准；

3）提供LDAP目录查询证书状态服务，符合LDAP v3标准。

6.1.4.9.2 服务可用性

程远未来最长24小时发布一次CRL。

程远未来的OCSP（在线证书状态查询）服务，对依赖方提供7×24小时服务。

6.1.4.9.3 可选特征

证书状态的其他可选服务方式为证书持有者利用程远未来指定的 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，进行证书状态的查询。

6.1.4.10 密钥生成、备份与恢复

6.1.4.10.1 签名密钥对生成

程远未来证书持有者必须使用国家密码管理局批准许可的设备生成签名密钥对，例如由密码机、密码卡、智能密码钥匙、IC卡等生成。证书持有者在选择这些设备前，应事先向程远未来咨询有关系统兼容和接受事宜。程远未来向证书持有者提供符合国家密码管理相关规定的智能密码钥匙作为证书持有者签名密钥对的生成

和存储设备。

程远未来一般不提供代为生成签名密钥对，如果用户书面申请并经程远未来批准，程远未来可以为申请者代为生成密钥对，并且承诺不保留私钥的副本，采取足够的措施保证密钥对的安全性、可靠性和唯一性，但是由于此密钥对的遗失、泄露等原因造成的损失，程远未来不承担任何责任与义务。

证书持有者签名密钥对的产生，必须遵循国家的法律政策规定。程远未来支持多种模式的签名密钥对产生方式，证书申请者可根据其需要进行选择密钥生成模块。但是不管何种方式，密钥对产生的安全性都应该得到保证。程远未来在技术、业务流程和管理上，已经实施了安全保密的措施。

证书持有者负有保护私钥安全的责任和义务，并承担由此带来的法律责任。

6.1.4.10.2 加密密钥对生成与恢复

程远未来证书持有者的加密密钥对由程远未来代证书持有者向国家认可的程远未来密钥管理中心（KMC）申请生成，并由程远未来密钥管理中心（KMC）进行管理。当证书持有者需要恢复加密密钥时，按照程远未来密钥管理中心（KMC）的规范、流程，接受证书持有者的申请，为证书持有者恢复相应的加密密钥。

6.1.4.10.3 加密私钥传送给证书持有者

由证书签发机构代替证书持有者对密钥管理中心提出加密密钥申请请求，密钥管理中心对产生的加密私钥使用证书持有者通讯密钥进行数字信封加密，以数据流的方式传送给证书签发机构，通过证书签发机构下载到证书持有者证书载体时，证书持有者使用自己的证书载体解密该私钥并存储。

6.1.4.10.4 公钥传送给证书签发机构

证书持有者的签名证书公钥通过安全通道，经注册机构传递到程远未来。

证书持有者的加密证书公钥，由程远未来密钥管理中心（KMC）通过安全通道传递到程远未来CA中心。

从注册机构（RA)到程远未来CA中心以及从程远未来密钥管理中心（KMC）到程远未来CA中心的传递过程中，采用国家密码管理局许可的通讯协议及密钥算法，保证了传输中数据的安全。

6.1.4.10.5 电子认证服务机构公钥传送给依赖方

依赖方可以从程远未来的网站下载根证书和CA证书，从而得到CA的公钥。

6.1.4.10.6 密钥的长度

SM2 CA证书和证书持有者证书的密钥长度均为256bit。RSA CA证书的密钥长度为2048bit，可签发密钥长度为RSA1024bit和RSA2048bit的证书持有者证书。

如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，程远未来将会完全遵从。

6.1.4.10.7 公钥参数的生成和质量检查

公钥参数必须使用国家密码管理局批准许可的加密设备和硬件介质生成。对于参数质量的检查，同样由通过国家密码管理局批准许可的加密设备和硬件介质进行，例如加密机、加密卡、智能密码钥匙、IC卡等。程远未来认为这些设备和介质内置的协议、算法等已经具备了足够的安全等级要求。

6.1.4.10.8 密钥使用目的

证书持有者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。

6.2 应用集成支持服务

6.2.1 证书应用接口程序

程远未来提供应用接口程序供应用系统集成和调用。证书应用接口程序符合《电子政务数字证书应用接口规范》，包括证书环境设置、证书解析、随机数生成、签名验证、加解密、时间戳以及数据服务接口等功能。

程远未来提供的证书应用接口程序支持Windows、AIX、Solaris、linux等多种系统平台，并提供C、C#、Java等多种接口形态，可通过com组件、java组件、ActiveX控件、Applet插件等多种形态提供服务。

6.2.2 证书应用方案支持

程远未来针对电子政务信息系统的实际业务需求，提供电子认证安全需求分析、电子认证法律法规、技术及服务体系的咨询服务，并根据电子政务信息系统的特点设计满足业务要求的电子认证及电子签名服务方案。

6.2.3 证书应用接口集成

程远未来具备面向各类应用的证书应用接口集成能力，并能够达到以下要求：

1.具备在多种应用环境下进行系统集成的技术能力，包括基于 B/S 应用模式(支持 Java、.NET asp 等开发语言)以及基于 C/S 应用模式（支持 C、VC 等开发语言）的系统集成能力。

2.提供满足不同应用系统平台的证书应用接口组件包，包括 com 组件、java 组

件、ActiveX 控件、Applet 插件等。

3.提供集成辅助服务，包括接口说明、集成手册、测试证书、集成示例、演示 DEMO 等。

6.3 信息服务

6.3.1 服务内容

根据政务部门对证书应用信息的管理及决策需求，程远未来提供证书发放和应用情况信息汇总及统计分析的信息管理服务，信息服务包括：

1.证书信息服务

程远未来 CA 系统中签发、更新的数字证书，可实时或定时与电子政务信息系统进行数据同步，实现将证书信息同步到电子政务信息系统中。程远未来提交的数据包括业务类型、认证机构身份标识、用户基本信息、用户证书信息等。

2.CRL 信息服务

程远未来在证书持有者证书签发时，通过目录服务器自动将该证书公布,CRL 发布周期为 24 小时，即在 24 小时内发布最新 CRL。备份保存时间不少于证书失效后 10 年。

3.服务支持信息服务

程远未来以页面和服务的形式提供查询服务，接口符合《电子政务数字证书应用接口规范》的要求。

4.决策支持信息服务

程远未来面向电子政务应用单位、政府监管机构提供决策支持信息，包括用户档案信息、投诉处理信息、客户满意度信息、服务效率信息等。

6.3.2 服务管理规则

程远未来在提供信息服务时，做好相关信息的隐私保障机制，实现信息保护对用户的承诺。程远未来对技术、客服等凡是能够接触用户信息的工作人员进行保密培训，并签署保密协议，严禁泄露或私自使用用户信息和业务信息。

1. 私有信息类型的敏感度

对于以下信息，程远未来按照日常安全保密制度严格执行：

1) 企业、政府主管单位、政府办公人员等的隐私信息；

2) 集成商、应用系统开发商、合作伙伴等的商业秘密；

3) 政府部门的敏感信息和工作秘密。

证书发行过程中涉及的用户申请信息都是敏感信息，而发布的证书和 CRL 信息不属于敏感信息。

2. 允许的私有信息收集

程远未来仅允许在证书发行和管理时才能收集私有信息，且只收集对发行和使用证书有用的私有信息。除了有特殊要求外，程远未来不收集更多的私有信息。

3. 允许的私有信息使用

程远未来承诺只使用在 CA 或 RA 中收集的私有信息。若在某项业务中开展证书应用而获得的私有信息，在使用时，必须获得该业务应用单位的许可。

4. 允许的个人信息发布

程远未来和注册机构仅能面向证书应用单位发布与之相关的私有信息，以协助证书应用单位进行证书业务管理。在特别紧急的情况下，程远未来经管理机构授权可发布私有信息。任何特定的私有信息发布应遵循相关法律和政策执行。

5. 所有者纠正私有信息的机会

程远未来允许用户在其证书生命周期内对其私有信息进行更正。

6. 对司法及监管机构发布私有信息

程远未来或注册机构在以下情况下，可执行将私有信息发给获得相应授权的人员：

1) 根据国家相关法律法规，为司法机关提供私有信息；
2) 在私有信息所有者同意的情况下，可将私有信息提供给相应授权的人员；
3) 按照明确的法定权限的要求或许可。

6.3.3 服务方式

程远未来的信息服务以页面或接口的形式面向应用系统或证书用户提供服务，接口符合《电子证书数字证书应用接口规范》的要求。

6.4 使用支持服务

6.4.1 服务内容

使用支持服务是程远未来面向证书使用用户（即证书申请者、证书持用者）及证书应用单位提供的一系列售后服务及技术支持工作。

服务内容包括：数字证书管理、数字证书使用、证书存储介质硬件设备使用、电子认证软件系统使用、电子认证服务支撑平台使用以及各类数字证书应用（如证书登录、证书加密、数字签名）等贯穿证书使用和应用过程中的所有问题。

6.4.1.1 面向证书持有者的服务支持

数字证书管理：包括数字证书的导入、导出，以及客户端证书管理工具的安装、使用、卸载等。

数字证书应用：基于数字证书的身份认证、电子签名、加解密等应用过程中出现的各种异常问题，如：证书无法读取、签名失败、证书验证失败等。

证书存储介质硬件设备使用：包括证书存储介质使用过程中出现的口令锁死、驱动安装、介质异常等。

电子认证服务支撑平台使用：为用户提供在程远未来的数字证书在线服务平台中使用的各类问题，如：证书更新失败、下载异常、无法提交撤销申请等。

6.4.1.2 面向应用提供方的服务支持

电子认证软件系统使用：提供受理点系统、注册中心系统、LDAP、OCSP、信息服务系统等系统的使用支持问题，如证书信息无法查询、数据同步失败、服务无响应等。

电子签名服务中间件的应用：解决服务中间件在集成时出现的各种情况，如客户端平台适用性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等。

6.4.2 服务能力

程远未来提供多种服务方式，包括热线服务、在线服务、现场服务等在程远未来官网上可查询相应的服务方式。

程远未来建立了完善的服务保障体系，包括建立专业的服务队伍、服务规范、知识库、服务跟踪系统、满意度调查、投诉受理等。服务保障体系应根据服务业务的变化及时更新。

6.4.2.1 热线服务

用户拨打程远未来的服务热线，客服人员根据用户的问题请求，协助用户处理。

6.4.2.2 在线服务

在线服务通过提供网络实时通讯系统、远程终端协助系统，以及在线帮助与传统模式的结合，满足用户多种服务帮助的需求。

网络实时通讯系统：用户通过在线帮助网站远程发起支持请求，网站客服人员能够第一时间同登陆网站的访客取得联系，进行交流。

远程终端协助系统：用户通过安装远程终端软件，可以通过互联网或者局域网向客户服务人员发起协助请求。由服务人员通过远程终端控制功能，实时检测用户的软件硬件环境，通过同屏显示指导、帮助用户解决应用故障。

在线帮助与传统模式的结合：将在线服务系统与电话服务结合，方便客户既可以打电话、也可以自助上网，随时查询自己的服务记录、请求处理状态、产品配置信息等等。

6.4.2.3 现场服务

根据用户的实际需求，由技术支持工程师上门现场为用户处理数字证书应

用中存在的问题。

6.4.2.4 满意度调查

通过多种用户可接受的调查方式进行客户回访，包括电话、WEB 网站、邮件系统、短信、传真等。向用户提供调查表格以供用户填写，调查表格应清晰载明此次回访的目的及内容。并将用户回访中产生的相关文档进行归档、保存。

6.4.2.5 投诉受理

向用户公布电子政务电子认证服务监管部门的投诉受理方式。可通过电话、网站平台、电子邮件、即时通讯工具等方式及时接受客户投诉，投诉受理过程中应记录投诉问题，并将结果及时反馈给用户。将投诉受理中产生的相关文档进行归档、保存。

6.4.2.6 培训

培训方式由程远未来与客户双方约定的形式开展。

培训内容主要包括：电子认证服务基础性技术知识、服务规范、证书应用集成规范及相关帮助文档、常见问题解答、操作手册等。

6.4.3 服务质量

程远未来坐席服务、在线服务、现场服务时间做到充分满足各类用户的需要。服务时间至少是 5 天*8 小时，热线电话服务时间是 7 天*24 小时不间断服务。程远未来设有专门的投诉受理热线，承诺在一个工作日内进行投诉处理；程远未来制定了用户培训意见反馈表，对培训效果进行评估，并做出相应处理，保证优质的客户服务质量。应对技术问题和技术故障按照一般事件、严重事件、重大事件进行分类，制定响应处理流程和机制，以确保服务的及时性和连续性。

6.5 安全保障

6.5.1 认证机构设施、管理和操作控制

6.5.1.1 物理控制

1. 程远未来所在的物理环境严格按照《证书认证系统密码及其相关安全技术规范》的要求实施，具有电磁屏蔽、消防、物理访问控制、入侵检测报警等相关措施，并取得了相关部门的检测证书。

2. 程远未来所有员工佩戴标识身份的工牌，工作人员需使用身份识别卡和指纹鉴定才能进出机房。

3. 所有门禁系统能够记录人员进出信息，记录信息能够保存六个月。

4. 针对不同的人员角色程远未来设置不同的访问权限，只有经过授权的人员才能进入相应的区域，非授权人员不能进入。

5. 程远未来采用双链路冗余供电线路和双链路网络线路。

6. 对于报废的存储介质，经过检查无残留信息后，通过物理损坏的方式进行销毁。

7. 程远未来办公场所有物理安全员不间断执勤，监控物理场地安全，每天有专人负责巡检机房设备。

6.5.1.2 操作过程控制

1. 可信角色

在程远未来提供的电子认证服务过程中，能从本质上影响证书的颁发、使用、管理和撤销等涉及密钥操作的职位都被程远未来视为可信角色。这些角色包括但不限于：密钥管理人员、系统管理人员、安全审计人员、业务受理人员及业务咨询人员等，具体岗位名称和要求以程远未来的岗位说明为准。

2. 每项任务需要的角色

程远未来在具体业务规范中对关键任务进行严格控制，敏感操作需要多个可信角色共同完成，例如：

♦密钥和密码设备的操作和存放：需要5个密钥分管员中的至少3个管理员共同完成 。

♦程远未来对与运行和操作相关的职能有明确的分工，贯彻互相牵制的安全机制，保证至少一人操作，一人监督记录。

3. 每个角色的识别与鉴别

所有程远未来的在职人员，必须通过认证后，根据作业性质和职位权限的需要，发放系统操作卡、门禁卡、登录密码、操作证书、作业账号等安全令牌。对于使用安全令牌的员工，程远未来系统将独立完整地记录其所有的操作行为。

4. 需要职责分割的角色

为保证系统安全，遵循可信角色分离的原则，即程远未来的可信角色由不同的人担任。

6.5.1.3 人员控制

6.5.1.3.1 资格、经历和无过失要求

程远未来员工的录取经过严格的审查，根据岗位需要增加相应可信任的员工，

建立了可信人员清单和全员清单。对于充当可信角色或其他重要角色的人员，需要具备相应的资格、经历和无过失要求。程远未来对承担可信角色的工作人员的资格要求如下：

1. 具备良好的社会和工作背景。

2. 遵守国家法律、法规，服从程远未来的统一安排及管理。

3. 遵守程远未来有关安全管理的规范、规定和制度。

4. 具有良好的个人素质、修养以及认真负责的工作态度和良好的从业经历。

5. 无违法犯罪记录。

程远未来要求充当可信角色的人员至少必须具备忠诚、可信赖及对工作的热诚、无影响 CA 运行的其它兼职工作、无同行业重大错误记录等。

6.5.1.3.2 背景审查程序

程远未来制定了严格的员工背景审查程序，与有关的政府部门和调查机构，完成对程远未来可信任员工的背景调查。

基本调查包括对工作经历、职业推荐、教育、社会关系方面的调查。

全面调查除包含基本调查项目外还包括对犯罪记录、社会关系和社会安全方面的调查。

调查程序包括：

a) 人事部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。

b) 人事部门通过电话、信函、网络、走访、等形式对其提供的材料的真实性进行鉴定。

c) 在背景调查中，对发现以下情形的人员，可以直接拒绝其成为可信人员的资格：

♦存在捏造事实或资料的行为；

♦借助不可靠人员的证明：

♦使用非法的身份证明或者学历、任职资格证明：

♦工作中有严重不诚实的行为。

d) 用人部门通过现场考核、日常观察、情景考验等方式对其考察。关键和核心岗位的人员通过录入考察期后，还需要额外期限的考察。根据考察的结果做出相应的安排。

e) 经考核，程远未来与员工签订保密协议，以约束员工不许泄露CA证书服务的所有保密和敏感信息。同时，程远未来还将按照本机构的人员管理相关条例对所有

承担可信角色的在职人员进行职位考察，以便能够持续验证这些人员的可信程度和工作能力。

6.5.1.3.3 培训要求

程远未来对程远未来员工进行以下内容的综合性培训：

1) 程远未来运营体系；

2) 程远未来技术体系；

3) 程远未来安全管理策略和机制；

4) 程远未来岗位职责统一要求；

5) PKI 基础知识；

6) 身份验证和审核策略和程序；

7) 程远未来电子政务电子认证服务业务规则；

8) 程远未来灾难恢复和业务连续性管理；

9) 程远未来管理政策、制度及办法等；

10) 国家关于电子认证服务的法律、法规及标准、程序；

11) 其他需要进行的培训等。

6.5.1.3.4 再培训周期和要求

根据程远未来策略调整、系统更新等情况，程远未来将对员工进行继续培训，以适应新的变化。对于公司安全管理策略，每年对员工进行一次以上的培训；对于相关业务技能培训应每年进行一次以上的业务技能培训。

6.5.1.3.5 工作岗位轮换周期和顺序

根据岗位人员和业务上的实际情况内部自行安排。

6.5.1.3.6 未授权行为的处罚

当程远未来员工进行了未授权或越权操作，程远未来在确认后将立即中止该员工进入程远未来证书服务体系，根据情节严重程度实施包括提交司法机关处理等措施。一旦发现上述情况，程远未来立即作废或终止该人员的安全令牌。

6.5.1.3.7 独立合约人的要求

程远未来的独立合约人及顾问执行与普通员工一致的可信资格确认，此外独立合约人及顾问进入关键区域必须有专人的陪同与监督。

6.5.1.3.8 提供给员工的文档

在培训或再培训期间，程远未来提供给员工的培训文档包括（但不限于）以下

几类：

1)员工手册；

2)电子政务电子认证服务业务规则；

3)岗位说明书；

4)安全管理制度等。

6.5.1.4 审计日志程序

程远未来建立了明确的审计日志程序：

- ◆ 确定CA中心的业务符合对CPS等文档中的定义。
- ◆ CA中心的管理人员需要定期对安全策略和操作流程的执行情况进行检查确认，进行运营风险评估。
- ◆ 必须准确完整地记录CA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。
- ◆ 各类日志、安全事件的记录在机密和公正的情况下以自动或手动方式产生，并定期归档。授权安全管理人员定期检阅记录和跟进有关事项。
- ◆ 建立检测CA系统访问的检测系统，保证非授权的访问能够被发现。

6.5.1.4.1 记录事件的类型

程远未来的CA和RA运行系统，记录所有与系统相关的事件，以备审查。这些记录，无论是纸质或电子文档形式，都包含事件日期、事件的内容、事件的发生时间段、事件相关的实体等。

6.5.1.4.2 审计日志的保存期限

程远未来会妥善保存认证服务的审计日志，本地保存期限至少三个月，离线存档为十年。

6.5.1.4.3 审计日志的保护

程远未来执行严格的保护和管理，确保只有程远未来授权的人员才能访问这些审查记录。并且实现异地备份，并禁止未授权的情况下访问、阅读、修改和删除等操作。

6.5.1.4.4 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都按照程远未来备份标准和程序进行。根据记录的性质和要求，采用在线和离线的各种备份工具，有实时、每天、每周、每月和每年等各种形式的备份。

6.5.1.4.5 审计收集系统

程远未来审查采集系统涉及：

1) 证书签发系统；
2) 证书注册系统；
3) 证书目录系统；
4) 访问控制系统（包括防火墙）；
5) 网站、数据库安全保障系统；
6) 其他程远未来认为有必要审查的系统。

6.5.1.4.6 对导致事件实体的通告

程远未来将依据法律、法规的监管要求，对一些恶意行为，如网络攻击等，通知相关的主管部门，并且程远未来保留进一步追究责任的权利。

6.5.1.4.7 脆弱性评估

CA 安全程序根据政策、技术和管理的变化及时进行薄弱环节分析，属于可以弥补的薄弱环节，及时弥补；属于不可弥补的薄弱环节，程远未来每年对系统进行脆弱性评估，以降低系统运行的风险。

6.5.1.5 记录归档

6.5.1.5.1 归档记录的类型

程远未来对下列记录（包括但不限于）进行归档保存：

1) 系统建设和升级文档；
2) 证书申请信息、证书服务批准和拒绝的信息、与证书证书持有者的协议、证书和CRL等；
3) 系统运行和认证服务产生的日志数据、认证系统证书密钥升级和更新信息等；
4) 电子认证服务规则、各类服务规范和运作协议、管理制度等；
5) 系统数据库数据；
6) 人员进出记录和第三方人员服务记录；
7) 监控录像；
8) 员工资料，包括背景调查、录用、培训等资料；
9) 各类外部、内部审查评估文档；
10) 审计数据；

6.5.1.5.2 归档记录的保存期限

除了法律法规和证书主管机构提出的保存期限以外，程远未来制订的有关第三方电子认证服务运营信息的归档保存期限至少应该如下：

1) 面向企事业单位、社会团体、社会公众的电子政务电子认证服务，信息保存期为证书失效后五年。
2) 面向政务部门的电子政务电子认证服务，信息保存期为证书失效后十年。

6.5.1.5.3 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能获取。程远未来保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力等的破坏。

6.5.1.5.4 归档文件的备份程序

所有纸质归档记录按照备份策略和流程由专人定期执行，备份介质在程远未来公司本地备份管理。按照备份策略和流程，电子存档文件除了在程远未来内本地备份外，还将在异地保存其备份。

6.5.1.5.5 记录时间戳要求

所有6.5.1.5.1条款所述的存档内容都按照归档策略和流程分别由专人收集、归档、审核和保管。所有归档记录上均有参与归档操作的人员与时间记录。

6.5.1.5.6 归档收集系统

程远未来的档案收集系统由人工操作和自动操作两部分组成。

6.5.1.5.7 获得和检验归档信息的程序

只有被授权的可信人员能够访问归档记录。所有记录被访问后，在归还时需验证其完整性。此外，程远未来每年验证存档信息的完整性。

6.5.1.6 认证服务机构密钥更替

认证机构进行密钥更替时应采用与初始化CA机构密钥相同的方式进行。

确保新旧密钥更替期间，认证机构CA密钥及信任链验证的有效性，避免对现有应用造成影响。新旧CA证书过渡时，必须采用新私钥为旧公钥签名证书、旧私钥为新公钥签名证书、新私钥为新公钥签名的证书方式，保证用户和依赖方能够可靠地验证CA机构证书以及确保证书信任链的有效性。

6.5.1.7 数据备份

程远未来建立数据备份管理机制，采用本地实时备份（Data Guard）、定时备份（EXP）、本地实时备份和异地定时备份相结合的方式备份重要数据库的数据。对关键系统数据，包括证书数据、系统配置数据、用户数据、审计日志数据和其他敏感信息进行异地备份，并确保其处于安全的设施。

程远未来建立了业务连续性计划和严格的备份管理策略，定期开展数据备份。

数据备份采用磁盘阵列、光盘等多种方式备份数据，具备快速恢复能力，保证系统数据和服务的连续性，减少对业务运营的影响。

6.5.1.8 损害与灾难恢复

6.5.1.8.1 事故和损害处理程序

遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，程远未来将按照灾难恢复计划实施恢复。具体由程远未来灾难恢复计划决定。

6.5.1.8.2 计算资源、软件或数据的损坏

程远未来对业务系统及其他重要系统的资源、软件和/或数据进行了备份，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，能在最短的时间内恢复被损害的资源、软件和/或数据。

6.5.1.8.3 实体私钥损害处理程序

对于实体私钥的损害，程远未来有如下处理要求和程序：

1）当证书持有者发现实体证书私钥损害时，证书持有者必须立即停止使用其私钥，并立即通知程远未来或注册机构撤销其证书。程远未来按CPS发布证书撤销信息。

2）当程远未来或注册机构发现证书证书持有者的实体私钥受到损害时，程远未来或注册机构将立即撤销证书，并通知证书持有者，证书持有者必须立即停止使用其私钥。程远未来按CPS发布证书撤销信息。

3）当程远未来的CA证书出现私钥损害时，程远未来将立即向国家密码管理局申请撤销CA证书并及时通过尽可能的途径通知依赖方。

6.5.1.8.4 灾难后的业务连续性能力

除非物理场地出现了毁灭性的、无法恢复的灾难，当发生灾难事故时，程远未来能够根据业务连续性计划进行数据恢复。程远未来目前正计划建立异地灾难恢复中心，灾难恢复中心的建立，将进一步增强程远未来的灾后业务存续能力。

6.5.1.8.5 业务连续性计划的保障方案

A. 建立CA中心的业务可持续性计划，并进行经常检查和更新，确保其持续有效。

B. 对CA系统中的重要部件制订完善的灾难恢复流程，并经常进行演练，确保流程操作的有效性。

C. 建立重要系统、数据、软件的备份，并存放在符合 CPS 要求的安全环境中，确保只有合理授权人员才可接触备份。

D. 定期测试备份设备、设施、后备电源等，确保其可用性。

E. 建立当CA签名密钥可信性受威胁时的应变计划。

F. 制订相关流程，对CA中心终止服务时的告知及业务承接作出计划。

6.5.1.9 认证服务机构或注册机构的终止

因各种情况，程远未来需要终止运营时，将严格按照《电子政务电子认证服务管理办法》的要求，处理好相关承接事项，包括档案记录管理者的身份问题。

6.5.2 认证系统技术安全控制

6.5.2.1 密钥对的生成和安装

1）CA 密钥对的产生

程远未来CA密钥对由专门的密钥管理员及若干名接受过相关培训的可信雇员在程远未来安全设施中按照规定的密钥生成规程进行产生。程远未来密钥生成、保存的密码模块符合国家密码主管部门的要求，并通过国家密码主管部门的鉴定。

2）最终证书持有者密钥对的产生

证书持有者签名证书使用密码模块（如 智能密码钥匙，智能卡）产生密钥对，加密证书的密钥由 KMC 产生，通过安全通道传递给证书持有者。

6.5.2.2 私钥保护和密码模块工程控制

程远未来私钥的生成、更新、撤销、备份和恢复等操作采用多人控制机制，即采取五选三方式，将私钥的管理权限分散到五位密钥管理员中，至少在其中三人在场并许可的情况下，插入管理员卡并输入 PIN 码，才能对私钥进行操作。

证书持有者的私钥由证书持有者自己通过密码设备控制，证书持有者有责任妥善保管私钥（签名证书）。

6.5.2.3 密钥对管理的其他方面

1、公钥归档

对于生命周期外的CA和证书持有者证书，程远未来将进行归档。归档的证书存

放在归档数据库中。

2、证书操作期和密钥对使用期限

证书操作期终止于证书过期或者被撤销。程远未来为证书持有者颁发的证书操作周期通常与密钥对的使用周期是相同的。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。为了保证能够验证在证书有效期内的签名的信息，公钥的使用期限可以在证书的有效期限外。

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。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。

6.5.2.4 激活数据

1、激活数据的产生和安装

存放有程远未来根密钥的加密卡的激活信息（秘密分割），其产生按程远未来密钥生成规程进行。所有秘密分割的创建和分发有相应的记录，包括产生时间、持有人等信息。

程远未来CA私钥的激活数据由硬件加密卡内部产生，并分割保存在5个智能卡中，需通过专门的读卡设备和软件读取。

如果证书持有者证书私钥的激活数据是口令，这些口令必须：

A. 由用户产生；

B. 至少8 位字符；

C. 至少包含一个字符和一个数字；

D. 至少包含一个小写字母；

E. 不能包含很多相同的字符；

F. 不能和操作员的名字相同；

G. 不能包含用户名信息中的较长的子字符串。

2、激活数据的保护

保存有程远未来CA私钥的激活数据的5个智能卡，由程远未来5个不同的密钥分管员掌管，而且密钥分管员必须符合程远未来职责分割的要求。

如果证书持有者使用口令或 PIN 码保护私钥，证书持有者应妥善保管好其口令或 PIN 码，防止泄露或窃取。

3、激活数据的其他方面

1).激活数据的传送

存有程远未来CA私钥的激活数据的智能卡，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的监督下进行。

当证书持有者证书私钥的激活数据需要进行传送时，证书持有者应保护它们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

2).激活数据的销毁

存有程远未来CA私钥的激活数据的智能卡，其销毁所采取的方法包括将智能卡初始化、或者彻底销毁智能卡，保证不会残留有任何秘密信息。CA私钥激活数据的销毁是在程远未来安全管理人员的监督下进行。

当证书持有者证书私钥的激活数据不需要时应该销毁，证书持有者应该确保无法通过残余信息、介质直接或间接恢复激活数据的部分或全部，比如记录有口令的纸页必须粉碎。

6.5.2.5 计算机安全控制

1、特别的计算机安全技术要求

程远未来系统的信息安全管理，按照国家密码管理局公布的《证书认证系统密码及其相关安全技术规范》、《电子政务电子认证服务管理办法》，参照IS017799信息安全标准规范以及其他相关的信息安全标准，制定出全面、完善的安全管理策略和制度，在运营中予以实施、审查和记录。主要的安全技术和控制措施包括：身份识别和验证、逻辑访问控制、物理访问控制、人员职责分权管理、网络访问控制等。

实行严格的双因素验证机制，为每位拥有系统（包括CA系统、RA系统）访问权限的人员分配唯一的账户，账户的访问权限限制为执行工作职责要求的最小权限。访问时同时采用数字证书及用户名和口令两种登录方式。

通过严格的安全控制手段，确保CA软件和数据文件的系统是安全可信的系统，不会受到未经授权的访问。

核心系统必须与其他系统物理分离，生产系统与其他系统逻辑隔离。这种分离可以阻止除指定的应用程序外对网络的访问。使用防火墙阻止从内网和外网入侵生产系统网络，限制访问生产系统的活动。只有CA系统操作与管理组中的、有必要工作需要、访问系统的可信人员可以通过口令访问CA数据库。

2. 计算机安全评估

程远未来根据法律法规和主管部门的规定，按照国家计算机安全等级的要求，实现安全等级制度。

程远未来的认证系统，通过了国家密码管理局的安全性审查。

程远未来的认证系统、计算机及网络安全，每年由国家密码管理局主管部门对认证系统、计算机、网络安全进行年度评估审查，并根据相关专家及领导意见，对认证系统及系统安全进行升级改造。

程远未来的CA系统及其运营环境通过了符合国家标准的检测。为全面贯彻公司“依法合规运营、确保信息安全、实现持续改进、提升客户满意”的信息安全方针，进一步提升服务质量，程远未来通过了ISO/IEC 27001现场审查。

6.5.2.6 生命周期技术控制

1、 CA 系统运行管理

程远未来每天由专人负责巡检机房设备的工作情况，定期由运维人员检查软件系统的运行情况。机房部署了漏洞扫描系统、入侵检测系统和防火墙等，以确保网络环境的安全稳定。

2、CA 系统的访问管理

设置关键岗位和职责分工，对于 CA 系统的访问权限进行严格限制，未授权人员不得访问 CA 系统。

3、 CA 系统的开发和维护

原则上不对 CA 系统进行技术开发和直接调用其数据，仅将 LDAP 和 RA系统对外提供查询和访问服务。

6.5.2.7 网络的安全控制

程远未来网络中有防火墙、入侵检测、漏洞扫描和网络防病毒等安全机制保护，其配置只允许已授权的机器访问。只有经过授权的程远未来员工才能够进入程远未来签发系统、注册系统、目录服务器、证书发布系统等设备或系统。所有授权用户必须有合法的安全令牌，并且通过密码验证。

CA系统只开放与申请证书、查询证书等相关操作功能，其他端口和服务全部关闭。CA系统的边界控制设备拒绝一切非电子认证业务的服务。

6.5.2.8 时间戳

程远未来认证系统的各种系统日志、操作日志有对应的记录时间。这些时间标识未采用基于密码的数字时间戳技术。

第七章 电子政务电子认证服务操作规范

7.1 数字证书服务操作规范

7.1.1 数字证书格式

程远未来提供的数字证书完全符合《基于SM2密码算法的数字证书格式规范》的要求。

7.1.2 身份标识与鉴别

1. 命名

程远未来提供的数字证书命名符合《基于SM2密码算法的数字证书格式规范》的要求，不使用匿名和假名。

2. 初始身份确认

1) 证明持有私钥的方法

程远未来通过以下方式证明证书持有者对私钥的持有：

（1）通过证书请求中所包含的数字签名来证明证书持有者持有与注册公钥对应私钥。

a) 证书持有者在客户端生成公私钥对；

b) 证书持有者使用私钥对证书请求信息签名，并连同公钥一同提交 CA 系统；

c) CA 使用证书持有者公钥验证证书持有者签名。

（2）证书持有者必须妥善保管自己的私钥，即只有证书持有者可以持有私钥。

如以上条件满足，则证书持有者可以被视作其私钥的唯一持有者。

2) 组织机构身份的鉴别

机构申请数字证书时，应按照程远未来的要求提交相应的证明文件及其复印件，包括：数字证书申请表、组织机构代码证、企业法人营业执照、经办人的有效身份证件、加盖公章的授权申请文件等。如需申请电子印章，还需要提交加盖公章的符合程远未来要求的印章图案。

程远未来有权对组织机构提交的证明材料进行验证和审核，若审核通过，程远未来将申请材料（证明材料、申请表）保存并归档保护。

3) 个人身份的鉴别

申请个人证书应提交个人合法身份证明文件及其复印件，或其它可用于身份真实性及一致性核验的身份证明文件。合法的身份证明文件包括身份证、护照、军官证、警官证、士兵证、士官证等。程远未来有权利对个人提交的所有证明文件进行审核和查验，如审核通过，程远未来将所有证明文件连同申请表一并归档保存。在把证书签发给政府部门个人时，还应进行以下鉴证工作：

a) 申请人提交由所属政府部门签章的证明文件，明确部门的名称并证明申请人属于该部门。

b) 程远未来对上述材料进行审核，做出批准申请或拒绝申请的操作。

c) 如批准申请，将保留该材料，并将申请表与其他证明文件一并归档保存。

3. 密钥更新请求的识别与鉴别

1） 常规密钥更新请求的识别与鉴别

对于一般正常情况下的密钥更新申请，证书持有者应提交能够识别原证书的足够信息，并使用更新前的私钥对包含新公钥的申请信息签名。对申请的鉴别满足以下条件：

a)密钥更新请求中，确保更新请求与申请者身份的关联和申请行为的有效性，采取现场受理和远程在线等方式对用户身份进行实体鉴别。

b)当用户证书已过期时，重新进行与初始身份确认相同的实体鉴别流程。

c)当用户证书未过期时，用户采取在线更新方式的，由用户在线提交更新申请并进行数字签名，以实现对用户身份的实体鉴别。

2） 撤销之后的密钥更新请求的识别与鉴别

程远未来不提供证书被撤销后的密钥更新服务。

4. 撤销请求的身份标识与鉴别

证书持有者本人申请撤销证书时的身份标识和鉴别采用与初始身份验证相同的流程。如果是因为证书持有者没有履行本 CPS 所规定的义务，由程远未来、注册机构申请撤销证书持有者的证书时，不需要对证书持有者身份进行标识和鉴别。

7.1.3 数字证书服务操作要求

7.1.3.1 证书申请

证书申请者提交证书申请时，应按照初始身份鉴别的要求，填写申请表，提交身份证明材料。程远未来将根据证书申请者提交的资料进行以下操作：

1) 对接收到申请材料进行通知；

2) 核查材料是否充分；

3) 验证证书申请信息的完整性；

4) 对申请材料保密；

5) 确认用户接受服务协议。

7.1.3.2 证书申请处理

程远未来在接收到证书申请后：

1) 按照初始身份鉴别的要求，对证书申请者的身份进行识别和鉴证；

2) 对证书申请者申请行为的合法性进行鉴证，确认申请行为得到合法授权；

3) 依据鉴证结果，做出接受或拒绝证书申请的决定。在 24 小时内，告知证书申请者结果及相应的原因。

4) 如接受申请，妥善保管证书申请者申请时提交的所有资料。

7.1.3.3 证书签发

1. 证书签发中 RA 和 CA 的行为

在证书的签发过程中RA的管理员负责证书申请的审批，并通过操作RA系统将签发证书的请求发往CA的证书签发系统。RA 发往CA的证书签发请求信息须有RA的身份鉴别与信息保密措施，并确保请求正确发送至CA证书签发系统。

CA 的证书签发系统在获得RA的证书签发请求后，对来自RA的信息进行鉴别与解密，对于有效的证书签发请求，证书签发系统签发证书持有者证书。

程远未来在批准证书申请之后，将签发证书。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

通常程远未来签发的证书在24小时内生效。

2. CA 和 RA 通知证书申请者证书的签发

如果证书申请获得批准并签发，RA 将通过多种方式告诉证书申请者如何获取证书。

程远未来对证书申请者的通告提供以下几种方式：

1) 电子或纸质的受理回执；

2) 电子邮件（e-mail）；

3) 通过面对面的方式，通知证书持有者（如申请者到受理点领取等方式）；

4) 其他程远未来认为安全可行的方式。

7.1.3.4 证书接受

1. 构成接受证书的行为

证书持有者接受证书的方式有如下几种：

A. 通过面对面的提交，证书持有者接受载有证书和私钥的介质。

B. 证书持有者通过网络将证书下载到本地存放介质。

完成以上行为表明证书持有者接受证书。在证书持有者接受到证书后，证书持有者应立即对证书进行检查和测试。

2. 电子认证服务机构对证书的发布

对于证书申请者明确表示拒绝发布证书信息的，程远未来不发布该证书申请者证书信息。没有明确表示拒绝的，程远未来将证书信息发布到目录系统。

程远未来采用主、从目录服务器结构来分布所签发证书。签发完成的数据直接发布到主目录服务器中，然后通过主从映射，将主目录服务器的数据自动同步到从目录服务器中，供证书持有者和依赖方查询和下载。

3. 电子认证服务机构对其他实体的通告

程远未来不具有向其他实体进行单独通告的义务，但使用证书的各类实体可以通过程远未来查询服务获得所需证书信息。

7.1.3.5 密钥对和证书使用

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

1. 证书持有者的私钥和证书使用

证书持有者只能在本 CPS 规定的应用范围内使用私钥和证书，对于签名证书，其私钥可用于对信息的签名，证书持有者应知悉并确认签名的内容。对于加密证书，其私钥可用于对采用对应公钥加密的信息进行解密。在证书到期或被撤销之后，证书持有者必须停止使用该证书对应的私钥。

2. 依赖方的公钥和证书使用

当依赖方接受到签名信息后，应该：

1) 获得对应的证书及信任链；

2) 验证证书的有效性；

3) 确认该签名对应的证书是依赖方信任的证书；

4) 证书的用途适用于相应的签名；

5) 使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。

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

7.1.3.6 证书更新

证书更新指在不改变证书注册信息的情况下，为证书持有者签发一张新证书。

1. 更新申请的提交证书持有者、证书持有者的授权代表或证书对应实体的拥有者在证书满足更新条件时，应按要求向程远未来提出更新申请。可采取当面提交更新申请表或在线提交带有证书持有者数字签名的更新申请。

2. 处理证书更新请求

程远未来将根据提交的申请进行处理，包括申请验证、鉴别、签发证书。对申请的验证和鉴别基于以下几个方面：

A. 申请对应的原证书存在并且由程远未来签发。

B. 用原证书上的证书持有者公钥对申请的签名进行验证。

C. 基于原注册信息，按照密钥更新时的要求，进行身份鉴别。

在以上验证和鉴别通过后才可以进行证书更新。

证书更新通过以下方式进行：

A. 面对面的更新方式；

B. 在线的自动更新方式。

3. 通知证书持有者新证书的签发

如果证书申请获得批准并签发，RA 将通过多种方式告诉证书申请者如何获取证书。

程远未来对证书申请者的通告提供以下几种方式：

1) 电子或纸质的受理回执；

2) 电子邮件（e-mail）；

3) 通过面对面的方式，通知证书持有者（如申请者到受理点领取等方式）；

4) 其他程远未来认为安全可行的方式。

4. 构成接受更新证书的行为

在程远未来数字证书签发完成后，程远未来将把数字证书当面或寄送给证书持有者，证书持有者从获得证书起就被视为已同意接受证书。证书持有者接受数字证书后，应妥善保存其证书对应的私钥。

5. CA 对更新证书的发布

对于证书申请者明确表示拒绝发布证书信息的，程远未来不发布该证书申请者证书信息。没有明确表示拒绝的，程远未来将证书信息发布到目录系统。

程远未来采用主、从目录服务器结构来分布所签发证书。签发完成的数据直接发布到主目录服务器中，然后通过主从映射，将主目录服务器的数据自动同步到从目录服务器中，供证书持有者和依赖方查询和下载。

6. CA 通知其他实体证书的签发。

程远未来不具有向其他实体进行单独通告的义务，但使用证书的各类实体可以通过程远未来查询服务获得所需证书信息。

7.1.3.7 证书撤销

1. 证书撤销的发起

程远未来认可以下实体发起的证书撤销请求：

A.程远未来、电子政务机构或依赖方在满足证书撤销条件的前提下，可以要求撤销一个证书持有者证书。

B. 对于个人证书，证书持有者可以请求撤销他们自己的个人证书。

C. 对于机构证书，只有机构授权的代表有资格请求撤销已经签发给机构的证书。

D. 对于设备证书，只有拥有该设备的机构授权的代表有资格请求撤销已经签发给该设备的证书。

2. 证书撤销的处理

A.程远未来在接到证书持有者的撤销请求后，通过核实身份证明材料、验证预留信息等方式，确认请求确实来自证书持有者。

B. 对于验证通过的请求，在 CA 系统中执行撤销证书操作，并在 24 小时内将撤销证书发布到证书撤销列表中。

C.程远未来在确信出现证书撤销条件的情况而需要立即撤销证书时，立即撤销证书。

D. 证书撤销后，通过电话、短信、网站等方式告知用户或依赖方证书撤销结果。

3. 依赖方检查证书撤销的要求

对于安全保障要求比较高并且完全依赖证书进行身份鉴别与授权的应用，依赖方在依赖一个证书前：

A. 应根据证书标明的发布地址获取证书撤销列表。

B. 应验证撤销列表的签名，确认其来是由程远未来 CA 签发的。

C. 应验证证书撤销信息，确认证书是否被撤销。

4. CRL 发布频率

程远未来的 CRL 发布周期为 24 小时，即在 24 小时内发布最新 CRL。但在特殊紧急情况下可以使 CRL 立即发布（假使网络传输条件能够保证），CRL 的立即生效由程远未来制定的发布策略决定。

CRL 结构如下：

A.版本号（version）

B.签名算法标识符（signature）

C.颁发者名称（issure）

D.本次更新（this update）

E.下次更新（next update）

F.用户证书序列号/撤销日期（user certificate/revocation date）

G.CRL 条目扩展项（crl entry extensions）

H.CRL 扩展域（crl extensions）

I. 签名算法（signature algorithm）

J. 签名（signature value）

5. CRL 发布的最大滞后时间

程远未来的 CRL 最大滞后时间不超过 24 小时。

6. 在线状态查询的可用性

程远未来提供在线查询服务（OCSP），OCSP 外网：

http://222.180.194.22:8013/ocsp/ocspcgic.cgi（电信）

http://113.204.229.146:8013/ocsp/ocspcgic.cgi（联通）

7. 在线状态查询要求

对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，依赖方在依赖一个证书前：

A. 应按照查询协议要求，向证书中标明的 OCSP 服务地址提交状态查询请求。

B. 查询过程应确保信息传输的机密性和完整性。

C. 应获得证书状态信息。

8. 撤销信息发布的其他形式

除了 CRL、OCSP 外，程远未来网站（http://www.ifutureca.com）提供CRL文件下载。

7.1.3.8 密钥生成、备份和恢复

证书持有者的签名密钥对由证书持有者的密码设备（如智能密码钥匙）生成和保管，加密密钥对由国家密码管理局批准建设的密钥管理中心提供密钥管理服务。

密钥恢复是指加密密钥的恢复，密钥管理基础设施不负责签名密钥的恢复。密钥恢复分为两类：证书持有者密钥恢复和问责取证密钥恢复。

1.证书持有者密钥恢复：当证书持有者的密钥损坏或丢失后，某些密文数据将无法还原，此时证书持有者可申请密钥恢复。证书持有者向程远未来提交申请，经审核后，通过程远未来 CA 系统向密钥管理基础设施发送请求，密钥恢复模块接受证书持有者的恢复请求，恢复证书持有者的密钥并下载到证书载体中。

2.问责取证密钥恢复：问责取证人员向密钥管理基础设施提交申请，经审核后，由密钥恢复模块恢复所需的密钥并记录于特定载体中。

7.2 应用集成支持服务操作规范

7.2.1 服务策略和流程

1.制定证书应用实施的管理策略和流程，针对不同政府行业的业务背景，程远未来会根据政府特点和不同要求进行充分调研，提供区分性的证书模板和接口文档、服务策略，指导或参与业务系统证书应用部分的开发和实施；

2.为确保项目交付时间和可交付物质量，程远未来会制定项目管理制度，规范项目规划、启动、实施及收尾行为，做好项目风险控制和时间、成本控制工作；

3.制定安全控制流程，明确人员职责；

4.实施证书软件发布版本管理，并进行证书应用环境控制；

5.项目开发程序和文档等资料妥善归档保存。

7.2.2 应用接口

程远未来的证书应用接口为上层提供简洁、易用的调用接口，主要包括密码设备接口和通用密码服务接口。

1. 密码设备调用接口

密码设备调用接口应包括服务器端密码设备的底层应用接口和客户端证书介质（如：智能密码钥匙）的底层应用接口。服务器端密码设备的底层应用接口符合国家相关技术规范，符合《公钥密码基础设施应用技术体系 密码设备应用接口规范》；客户端证书介质的底层应用接口符合《智能 IC 卡及智能密码钥匙密码应用接口规范》。

2. 通用密码服务接口

通用密码服务接口是屏蔽了底层不同密码设备类型和底层接口的通用中间件，该接口符合《电子政务数字证书应用接口规范》，主要包括服务器端组件接口和客户端控件接口。

3.密码模块安全技术接口

采用新模式与新技术密码模块安全技术接口，应符合 GM/T 0028 和 GM/T 0054 的要求。

7.2.3 集成内容

程远未来为电子政务应用单位提供证书应用接口程序集成工作。集成工作提供以下服务：

1. 证书应用接口的开发包；
2. 接口说明文档；
3. 集成演示 Demo；
4. 集成手册；
5. 证书应用接口开发培训和集成技术支持；
6. 协助应用系统开发商完成联调测试工作。

7.3 信息服务规范

7.3.1 服务内容

1.证书信息服务

CA 系统中签发、更新、撤销的数字证书，可实时或定时与电子政务信息系统进行数据同步，实现将证书信息同步到电子政务信息系统中。程远未来提交的数据包括业务类型、程远未来身份标识、用户基本信息、用户证书信息等。

2. CRL 信息服务

CRL 在 CA 系统中发布后，可实现将 CRL 实时发布到指定的电子政务信息系

统中。程远未来提交的数据包括业务类型、程远未来身份标识、CRL 文件、同步时间等。

3.服务支持信息服务

程远未来面向电子政务用户、应用系统集成商、应用系统发布与之相关的服务信息，包括 CPS、FAQ、证书应用接口软件包等。

4.决策支持信息服务

程远未来面向电子政务用户、政府监管机构提供决策支持信息，包括用户档案信息、投诉处理信息、客户满意度信息、服务效率信息等。

7.3.2 服务管理规则

1. 对 CA 机构内的工作人员按其工作角色设定与之相应的信息访问权限，并对其所有访问操作进行详细记录。

2. 对证书应用单位的管理员设定信息访问权限，限定其仅能访问本应用所签发证书信息。

3. 应用单位管理员对非授权信息的访问，依照政策管理规定，经上级主管部门批准后进行。

4.对问责程序需要进行的信息访问，严格审核相应的问责人员身份及授权文件，无误后进行问责举证。

5.对监管部门应管理需求进行的信息访问，按照相关的管理规定和调取程序，为其提供信息访问权限。

7.3.3 服务方式

1.证书信息同步服务

证书信息同步通过采用 webservice 技术实现 CA 系统与电子政务信息系统的证书应用同步。电子政务信息系统通过部署统一的 webservice 接口，程远未来的 CA 系统通过调用统一的 webservice 同步接口，实现 CA 系统向电子政务信息系统进行证书信息的自动同步功能。同时，为了保证数据传输的安全性，可通过 webservice 通信数据添加数字签名，以防止数据在传输中被篡改或数据损坏。

2. CRL 信息同步服务

CRL 信息同步服务通过采用 webservice 技术实现 CA 系统与电子政务信息系统的 CRL 同步。CA 系统主动调用该接口，实时将最新的 CRL 文件同步到电子政务信息系统中。 为了提高 CRL 文件传输的安全性，对发送 CRL 数据进行数字签

名，电子政务信息系统只需要根据 iFutureCA 身份标识找到对应的 CA 证书链，验证 CRL 签名的有效性即可确定 CRL 的有效性。

3.服务支持信息服务

程远未来通过 WEB 网站面向电子政务用户发布如下信息：

1) 电子政务电子认证服务业务规则
2) 证书生命周期服务流程
3) 证书用户操作手册
4) 证书常见问题解答（FAQ）
5) 获得证书帮助联系方式（客服电话、办公地址、邮政编码、投诉电话等）

程远未来通过 WEB 网站面向电子政务应用系统集成商发布如下信息：

1) 证书常见问题解答（FAQ）
2) 获得证书帮助联系方式（客服电话、办公地址、邮政编码、投诉电话等）

程远未来通过 WEB 网站面向电子政务应用系统发布如下信息：

1) http 协议的 CRL 发布服务接口
2) LDAP 协议的 CRL 发布接口
3) LDAP 协议的证书发布接口
4) OCSP 服务接口（可选）

4.决策支持信息服务

程远未来面向应用提供如下信息服务：

1) 用户档案信息：分业务、地域、时段等要素提供用户信息的统计分析服务；
2) 投诉处理信息：提供特定业务、时间、特定用户群、问题类型等的投诉处理汇总信息及分析；
3) 客户满意度信息：提供面向业务的客户满意度调查信息；
4) 服务效率信息：提供面向业务的服务效率分析信息，如处理时间、服务接通率等。

7.4 使用支持服务操作规范

7.4.1 服务内容

1.面向证书持有者的服务支持

A.数字证书管理

包括数字证书的导入、导出，以及客户端证书管理工具的安装、使用、卸载等。

B.数字证书应用

基于数字证书的身份认证、电子签名、加解密等应用过程中出现的各种异常问题，如：证书无法读取、签名失败、验签失败等。

C.证书存储介质硬件设备使用

包括证书存储介质使用过程中出现的 PIN 码锁死、驱动安装、介质异常等。

D.电子认证服务支撑平台使用

为用户提供数字证书在线服务平台中使用的各类问题，如：证书更新失败、下载异常、无法提交注销申请等。

2.面向应用提供方的服务支持

A.电子认证软件系统使用

提供受理点系统、注册中心系统、LDAP、OCSP、信息服务系统等的使用

支持问题，如证书信息无法查询、数据同步失败、服务无响应等。

B.电子签名服务中间件的应用

解决服务中间件在集成时出现的各种情况，如客户端平台适应性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等。

7.4.2 服务方式

程远未来提供多种服务方式，包括热线服务 023-63063149、在线服务（QQ：2686158304）、现场服务等在程远未来官网上可查询相应的服务方式。

程远未来建立了完善的服务保障体系，包括建立专业的服务队伍、服务规范、知识库、服务跟踪系统、满意度调查、投诉受理等。服务保障体系应根据服务业务的变化及时更新。

7.4.3 服务质量

程远未来坐席服务、在线服务、现场服务时间做到充分满足各类用户的需要。服务时间至少是 5 天*8 小时，热线电话服务时间是 7 天*24 小时不间断服务。程远未来设有专门的投诉受理热线 023- 67302734，承诺在一个工作日内进行投诉处理；程远未来制定了用户培训意见反馈表，对培训效果进行评估，并做出相应处理，保证优质的客户服务质量。应对技术问题和技术故障按照一般事件、严重事件、重大事件进行分类，制定响应处理流程和机制，以确保服务的及时性和连续性。

7.5 安全保障规范

7.5.1 认证机构设施、管理和操作控制

7.5.1.1 物理控制

程远未来电子认证服务机构的物理环境满足以下安全要求：

为防止物理非法进入，程远未来通过入侵报警、视频监控等安防设施对定义的管理区域进行实时监测，并建立完善的安全管理制度，保护程远未来的电子认证服务设施。

防止未授权访问，程远未来通过门禁系统和权限分割的管理模式，确保不发生未经过授权或越权的区域访问。

7.5.1.1.1 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》。

7.5.1.1.2 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，授权人员进出每一道门都会有记录，所有的录像资料根据安全审计要求保留一段时间。

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。

7.5.1.1.3 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。

7.5.1.1.4 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。

7.5.1.1.5 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，然后拨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。

7.5.1.1.6 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）。

7.5.1.1.7 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。

7.5.1.1.8 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。

7.5.1.1.9 入侵侦测报警系统

机房区域安装了入侵侦测报警系统，进行安全布防。机房区域、办公区域、公共区域、档案室、室外等各区域安装了 22 路高清摄像头，并启用了移动侦测报警功能。

7.5.1.2 操作过程控制

1、可信角色

在程远未来提供的电子认证服务过程中，能从本质上影响证书的颁发、使用、管理和撤销等涉及密钥操作的职位都被程远未来视为可信角色。这些角色包括但不限于：密钥和密码设备的管理员、系统管理员、安全审计人员、业务管理人员及业务操作人员等，具体岗位名称和要求以程远未来的岗位说明书为准。

2、每项任务需要的角色

程远未来确保单个角色不能接触、导出、恢复、更新、废止程远未来的 CA 系存储的 CA 证书对应的私钥。对于关键的操作进行物理与逻辑上的分割控制，使掌握设备物理权限的人不能再拥有逻辑权限。至少由 5 个密钥分管员中的 3 个管理员同时在场才能完成密钥分割和合成技术来进行任何钥匙恢复的操作。

程远未来对与运行和操作相关的职能有明确的分工，贯彻互相牵制的安全机制，保证至少一人操作，一人监督记录。

3、每个角色的识别与鉴别

所有程远未来的在职人员，必须通过认证后，根据作业性质和职位权限的需要，发放系统操作卡、门禁卡、登录密码、操作证书、作业账号等安全令牌。对于使用安全令牌的员工，程远未来系统将独立完整地记录其所有的操作行为。

所有程远未来职位人员必须确保：

1) 根据岗位安全等级的不同，进行不同程度层次的身份识别和鉴别措施；
2) 基本的身份审查措施，确保符合岗位可信资格；
3) 赋予可信员工相应的权限区分，为其发放安全令牌；
4) 发放的安全令牌只直接属于个人或组织所有；
5) 发放的安全令牌不允许共享。程远未来的系统和程序通过识别不同的令牌，对

操作者进行权限控制。

4、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。程远未来对如下人员进行了职责分割：

（1）安全管理员：

岗位职责：

1）负责制定、发布、废止、批准、实施CA机构总体信息安全策略、安全管理制度，并监督、检查安全运营和生产活动；

2）制定可信雇员管理策略并监督执行；

3）组织进行安全运营审计，发布审计报告；

（2）密钥管理员：

岗位职责：

1）为电子认证机构及客户创建并维护电子认证密钥对和证书；

2）建立密码硬件设备的采购、使用、测试、维修、保管、报废等管理制度，维护所有密钥相关设备的安全可靠；

3）协助电子认证密钥对的恢复工作；

4）建立当电子认证密钥对可信性受威胁时的应变计划。

5）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。

（3）证书申请录入员：

岗位职责：用户提交办理CA数字证书，提交申请资料，录入系统；通过系统将用户资料制作数字证书。

（4）证书申请鉴证员：

岗位职责：审核用户申请CA证书提交的资料，不通过给出反馈意见。

（5）档案管理员：

岗位职责：负责建立和维护客户档案资料，管理客户档案借阅工作等。

（6）系统维护人员：

岗位职责：

1）硬件故障的排查及维修等；

2）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；

3）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；

4）建立并执行系统故障报告、处理流程。

7.5.1.3 人员控制

7.5.1.3.1 资格、经历和无过失要求

程远未来员工的录取经过严格的审查，根据岗位需要增加相应可信任的员工，建立了可信人员清单和全员清单。

一般员工需要有3个月的考察期，核心和关键部位的员工考察期为半年，根据考察的结果安排相应的工作或者辞退。程远未来根据需要对员工进行职责、岗位、技能、政策、法律、安全等方面的培训。

程远未来会对其关键的CA职员进行严格的背景调查。背景调查主要通过（但不限于）以下方式：

1）身份验证，包括个人身份证件、户籍证件等；

2）学历、学位等其他资格、资历证书；

3）个人履历，包括家庭状况、教育经历、工作经历及相关证明人等；

4）无犯罪记录证明材料；

注册机构、注册分支机构和受理点操作员的审查，参照程远未来对可信任员工的考察方式。受理点责任机构在此基础上增加考察和培训条款，但不得违背程远未来电子政务电子认证服务业务规则。

程远未来确立流程管理规则，所有的员工与程远未来签订保密协议，据此CA员工受到合同和章程的约束，不得泄露程远未来证书服务体系的敏感信息。

7.5.1.3.2 背景审查程序

程远未来制定了严格的员工背景审查程序，与有关的政府部门和调查机构，完成对程远未来可信任员工的背景调查。身份背景调查过程中，存在（但不限于）下列情形之一，不得通过可信审查：

1）伪造相关证件材料的

2）伪造工作经历及工作证明人虚假的；

3）虚假声称具有某种技能、能力的证件；

4）以往工作中存在重大不诚实行为的；

5）有犯罪记录的。

7.5.1.3.3 培训要求

程远未来对程远未来员工进行以下内容的综合性培训：

1) 程远未来运营体系；

2) 程远未来技术体系；

3) 程远未来安全管理策略和机制；

4) 程远未来岗位职责统一要求；

5) PKI 基础知识；

6) 身份验证和审核策略和程序；

7) 程远未来电子政务电子认证服务业务规则；

8) 程远未来灾难恢复和业务连续性管理；

9) 程远未来管理政策、制度及办法等；

10) 国家关于电子认证服务的法律、法规及标准、程序；

11) 其他需要进行的培训等。

7.5.1.3.4 再培训周期和要求

根据程远未来策略调整、系统更新等情况，程远未来将对员工进行继续培训，以适应新的变化。对于公司安全管理策略，每年对员工进行一次以上的培训；对于相关业务技能培训应每年进行一次以上的业务技能培训。

7.5.1.3.5 工作岗位轮换周期和顺序

根据岗位人员和业务上的实际情况内部自行安排。

7.5.1.3.6 未授权行为的处罚

当程远未来员工进行了未授权或越权操作，程远未来在确认后将立即中止该员工进入程远未来证书服务体系，根据情节严重程度实施包括提交司法机关处理等措施。一旦发现上述情况，程远未来立即作废或终止该人员的安全令牌。

7.5.1.3.7 独立合约人的要求(含对外包服务方管理要求)

程远未来的独立合约人及顾问执行与普通员工一致的可信资格确认，此外独立合约人及顾问进入关键区域必须有专人的陪同与监督。

对外包服务方提出安全与控制要求参考以上执行。

7.5.1.3.8 提供给员工的文档

在培训或再培训期间，程远未来提供给员工的培训文档包括（但不限于）以下几类：

1)员工手册；

2)电子政务电子认证服务业务规则；

3)岗位说明书；

4)安全管理制度等。

7.5.1.4 审计日志程序

7.5.1.4.1 记录事件的类型

程远未来的CA和RA运行系统，记录所有与系统相关的事件，以备审查。这些记录，无论是纸质或电子文档形式，都包含事件日期、事件的内容、事件的发生时间段、事件相关的实体等。

程远未来应记录的内容包括（但不限于）：

1）系统安全事件，包括：CA系统、RA系统和其他服务系统的活动，对于CA系统网络的非授权访问及访问企图，系统崩溃，硬件故障和其他异常。

2）电子认证服务系统操作事件，包括系统的启动和关闭。

3）认证机构设施的访问，包括授权人员进出认证机构设施、非授权人员进入认证机构设施及陪同人和安全存储设施的访问。

4）证书生命周期内的管理事件，包括证书的申请、批准、更新、撤销等

7.5.1.4.2 审计日志的保存期限

程远未来会妥善保存认证服务的审计日志，本地保存期限至少三个月，离线存档为十年。

7.5.1.4.3 审计日志的保护

程远未来执行严格的保护和管理，确保只有程远未来授权的人员才能访问这些审查记录。并且实现异地备份，并禁止未授权的情况下访问、阅读、修改和删除等操作。

7.5.1.4.4 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都按照程远未来备份标准和程序进行。根据记录的性质和要求，采用在线和离线的各种备份工具，有实时、每天、每周、每月和每年等各种形式的备份。

7.5.1.4.5 审计收集系统

程远未来审查采集系统涉及：

7) 证书签发系统；

8) 证书注册系统；

9) 证书目录系统；

10) 访问控制系统（包括防火墙）；

11) 网站、数据库安全保障系统；

12) 其他程远未来认为有必要审查的系统。

7.5.1.4.6 对导致事件实体的通告

程远未来将依据法律、法规的监管要求，对一些恶意行为，如网络攻击等，通知相关的主管部门，并且程远未来保留进一步追究责任的权利。

7.5.1.4.7 脆弱性评估

CA 安全程序根据政策、技术和管理的变化及时进行薄弱环节分析，属于可以弥补的薄弱环节，及时弥补；属于不可弥补的薄弱环节，程远未来每年对系统进行脆弱性评估，以降低系统运行的风险。

7.5.1.5 记录归档

7.5.1.5.1 归档记录的类型

程远未来对下列记录（包括但不限于）进行归档保存：

1) 系统建设和升级文档；

2) 证书申请信息、证书服务批准和拒绝的信息、与证书证书持有者的协议、证书和CRL等；

3) 系统运行和认证服务产生的日志数据、认证系统证书密钥升级和更新信息等；

4) 电子认证服务规则、各类服务规范和运作协议、管理制度等；

5) 系统数据库数据；

6) 人员进出记录和第三方人员服务记录；

7) 监控录像；

8) 员工资料，包括背景调查、录用、培训等资料；

9) 各类外部、内部审查评估文档；

10) 审计数据；

7.5.1.5.2 归档记录的保存期限

除了法律法规和证书主管机构提出的保存期限以外，程远未来制订的有关第三方电子认证服务运营信息的归档保存期限至少应该如下：

1) 面向企事业单位、社会团体、社会公众的电子政务电子认证服务，信息保存期为证书失效后五年。

2) 面向政务部门的电子政务电子认证服务，信息保存期为证书失效后十年。

7.5.1.5.3 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能获取。程远未来保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力等的破坏。

7.5.1.5.4 归档文件的备份程序

所有纸质归档记录按照备份策略和流程由专人定期执行，备份介质在程远未来公司本地备份管理。按照备份策略和流程，电子存档文件除了在程远未来内本地备份外，还将在异地保存其备份。

7.5.1.5.5 记录时间戳要求

所有7.5.1.5.1条款所述的存档内容都按照归档策略和流程分别由专人收集、归档、审核和保管。所有归档记录上均有参与归档操作的人员与时间记录。

7.5.1.5.6 归档收集系统

程远未来的档案收集系统由人工操作和自动操作两部分组成。

7.5.1.5.7 获得和检验归档信息的程序

只有被授权的可信人员能够访问归档记录。所有记录被访问后，在归还时需验证其完整性。此外，程远未来每年验证存档信息的完整性。

7.5.1.6 电子认证服务机构密钥的更替

认证机构进行密钥更替时应采用与初始化CA机构密钥相同的方式进行。

确保新旧密钥更替期间，认证机构CA密钥及信任链验证的有效性，避免对现有应用造成影响。新旧CA证书过渡时，必须采用新私钥为旧公钥签名证书、旧私钥为新公钥签名证书、新私钥为新公钥签名的证书方式，保证用户和依赖方能够可靠地验证CA机构证书以及确保证书信任链的有效性。

7.5.1.7 数据备份

程远未来建立数据备份管理机制，采用本地实时备份（Data Guard）、定时备份（EXP）、本地实时备份和异地定时备份相结合的方式备份重要数据库的数据。对关键系统数据，包括证书数据、系统配置数据、用户数据、审计日志数据和其他

敏感信息进行异地备份，并确保其处于安全的设施。

程远未来建立了业务连续性计划和严格的备份管理策略，定期开展数据备份。

数据备份采用磁盘阵列、光盘等多种方式备份数据，具备快速恢复能力，保证系统数据和服务的连续性，减少对业务运营的影响。

1 备份内容

1) 主机操作系统；
2) 系统应用软件，如 Web 服务程序、数据库系统等；
3) 运营系统软件；
4) 系统配置；
5) 数据库用户数据。

2 备份策略

1) 采用专门的备份服务器对整个运营系统的软件及数据进行备份，备份数据保存在硬盘上；
2) 备份策略采用热备方式，备份保存于本地硬盘系统及光盘；
3) 备份策略保证没有数据丢失或数据丢失不会造成实质性的影响；
4) 在系统出现故障、灾难时，备份方案能够在最短的时间内从备份数据中恢复出原系统及数据；
5) 选择的备份介质能保证数据的长期可靠；
6) 对备份数据收集、保管、恢复进行管控，确保备份数据的安全，防止泄露和未经授权使用；
7) 定期检查备份系统和设备的可靠性和可用性，定期检查备份介质可靠性和数据完整性；
8) 每半年对系统数据备份进行测试检查，确保其可用性，每月进行一次备份数据库可用性恢复测试检查，确保系统备份数据库可用性。

7.5.1.8 损害和灾难恢复

7.5.1.8.1 事故和损害处理程序

遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，程远未来将按照灾难恢复计划实施恢复。具体由程远未来灾难恢复计划决定。

7.5.1.8.2 计算资源、软件或数据的损坏

程远未来对业务系统及其他重要系统的资源、软件和/或数据进行了备份，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，能在最短的时间内恢复被损害的资源、软件和/或数据。

7.5.1.8.3 实体私钥损害处理程序

对于实体私钥的损害，程远未来有如下处理要求和程序：

1）当证书持有者发现实体证书私钥损害时，证书持有者必须立即停止使用其私钥，并立即通知程远未来或注册机构撤销其证书。程远未来按CPS发布证书撤销信息。

2）当程远未来或注册机构发现证书证书持有者的实体私钥受到损害时，程远未来或注册机构将立即撤销证书，并通知证书持有者，证书持有者必须立即停止使用其私钥。程远未来按CPS发布证书撤销信息。

3）当程远未来的CA证书出现私钥损害时，程远未来将立即向国家密码管理局申请撤销CA证书并及时通过尽可能的途径通知依赖方。

7.5.1.8.4 灾难后的业务连续性能力

除非物理场地出现了毁灭性的、无法恢复的灾难，程远未来能够在出现灾难后最短时间内恢复其业务能力。程远未来目前正计划建立异地灾难恢复中心，灾难恢复中心的建立，将进一步增强程远未来的灾后业务存续能力。

7.5.1.8.5 业务连续性计划的保障方案

A. 建立CA中心的业务可持续性计划，并进行经常检查和更新，确保其持续有效。

B. 对CA系统中的重要部件制订完善的灾难恢复流程，并经常进行演练，确保流程操作的有效性。

C. 建立重要系统、数据、软件的备份，并存放在符合 CPS 要求的安全环境中，确保只有合理授权人员才可接触备份。

D. 定期测试备份设备、设施、后备电源等，确保其可用性。

E. 建立当CA签名密钥可信性受威胁时的应变计划。

F. 制订相关流程，对CA中心终止服务时的告知及业务承接作出计划。

7.5.1.9 认证机构或注册机构终止

与认证机构或注册机构终止和终止通告相关的过程，按照《电子政务电子认证

服务管理办法》的要求，处理好相关承接事项，包括认证机构或注册机构档案记录管理者的身份问题。

认证机构拟暂停或者终止认证服务的，在暂停或者终止认证服务六十个工作日前，选定业务承接认证机构，就业务承接有关事项作出妥善安排，并在暂停或者终止认证服务四十五个工作日前向国家密码管理局报告。

不能就业务承接事项作出妥善安排的，在暂停或者终止认证服务六十个工作日前，向国家密码管理局提出安排其他认证机构承接业务的申请。

7.5.2 认证系统技术安全控制

7.5.2.1 密钥对的生成与安装

由于密钥对是安全机制的关键，所以在电子政务电子认证服务业务规则中制定了相应的规定，通过物理安全控制和密钥安全存储控制来确保密钥对的产生、传送、安装等过程中符合保密性、完整性和不可否认性的需求。

7.5.2.1.1 密钥对的生成

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。

用户的加密密钥对是由国家密码管理局许可的密钥管理中心生成。

用户的签名密钥对是由客户端产生，证书申请者可使用密码管理局认可的、程远未来数字证书签发系统支持的介质生成签名密钥对。签名密钥存储在介质中不可导出，保证程远未来无法复制签名密钥对。程远未来支持多种介质，如智能密码钥匙、智能 IC 卡等。程远未来可根据证书申请者要求或自身选择签名密钥对生成介质。

服务器证书的密钥对由证书持有者自己产生，证书持有者应妥善保管。程远未来通过物理安全控制和密钥安全存储控制，在技术、流程和管理上保证密钥对产生的安全性。

7.5.2.1.2 加密私钥传送给证书持有者

证书持有者的加密私钥是在 KMC 产生的。在加密私钥从 KMC 到证书持有者的传递时，采用国家密码管理局许可的对称密钥算法加密，程远未来无法获得，这样就保证了证书持有者加密私钥的安全。

7.5.2.1.3 公钥传送给证书签发机构

程远未来从 KMC 取得证书持有者加密公钥后为其签发证书，在此过程中采用符合标准的安全协议进行传递，保证了传输中密钥的安全。自生成密钥对证书持有者向程远未来提交证书申请时，该请求信息内的公钥，使用安全通道保证信息的机密性和完整性。

电子认证服务机构 CA 公钥传送给依赖方，程远未来 CA 公钥包含在程远未来的 CA 证书中。证书持有者可以从程远未来的网站（http://www.ifutureca.com）上下载程远未来 CA 证书，也可以由程远未来通过目录系统、业务系统的安装、电子邮件和软件绑定等方式提供给依赖方。

7.5.2.1.4 密钥的长度

为了保证加密/解密的安全性，程远未来所使用的 SM2 算法密钥对长度为 256 位。如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，程远未来将会完全遵从。

7.5.2.1.5 公钥参数的生成和质量检查

公钥参数由国家密码管理局许可、程远未来数字证书签发系统支持的硬件生成。

7.5.2.1.6 密钥使用用途

在程远未来证书服务体系中的密钥用途和证书类型紧密相关，被分为签名和加密两大类。

程远未来的CA签名密钥用于签发用户证书和证书撤销列表（CRL）；

证书持有者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、授权管理和贵任认定等安全机制。

7.5.2.2 私钥保护和密码模块工程控制

7.5.2.2.1 密码模块的标准和控制

程远未来使用国家密码管理局许可的产品，密码产品的标准符合国家规定的要求。

7.5.2.2.2 私钥多人控制（m 选 n）

程远未来采用多人控制策略激活、使用、备份、停止和恢复程远未来的签名密钥，采取5个管理人员中至少3个在场才可进行操作的原则。

7.5.2.2.3 私钥托管

KMC根据客户和法律的需要，对加密密钥进行托管。签名私钥由证书持有者自己保管。

7.5.2.2.4 私钥备份

程远未来对其CA签名私钥通过专门的备份加密卡进行备份，私钥的备份采用多人控制策略。KMC备份托管的证书持有者加密私钥加密存储，确保加密私钥的安全。

7.5.2.2.5 私钥归档

KMC提供过期的托管私钥的存档服务；保存期为十年。当私钥过了保存期，将依据相关规定对其进行销毁。

7.5.2.2.6 私钥导入、导出密码模块

程远未来的CA私钥在硬件密码模块上生成、保存和使用。程远未来对CA私钥进行严格的密钥管理和备份、恢复控制，有效防止了CA私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

程远未来不提供证书持有者私钥从硬件密码模块中导出的方法，也不允许如此操作。对于存放在软件密码模块中的私钥，如果证书持有者愿意并且自行承担相关风险，证书持有者可自主选择导入导出的方式，操作时需要采用口令保护等授权访问控制措施。

7.5.2.2.7 私钥在密码模块的存储

程远未来私钥以加密的形式存放在硬件密码设备中，并在该设备中使用。

7.5.2.2.8 激活私钥的方法

程远未来将证书持有者证书的私钥保存在USB Key或智能卡等硬件密码模块中，只有输入PIN码，私钥才能被激活使用。

程远未来所签发的服务器类证书，证书的私钥由专有的密码模块提供和保存，当服务程序要加载私钥时需求通过保护口令的验证才能访问密码模块中的私钥。

7.5.2.2.9 解除私钥激活状态的方法

对于存放在密码模块中的证书的私钥，当密码模块被下载、证书持有者退出登录状态、操作关闭或计算机断电时，私钥被解除激活状态。

7.5.2.2.10 销毁私钥的方法

如果CA私钥不再被使用，或者与私钥相对应的公钥到期或者被撤销后，如果其处于软件加密模块内，那么该软件加密模块必须以被覆盖方式清除；如果位于硬件加密模块内，那么加密设备或者IC卡等必须被清空为零。同时，所有用于激活私钥的PIN码、IC卡等也必须被销毁或者收回。

对于程远未来签发的证书持有者加密证书私钥，在其生命周期结束后，KMC对该密钥进行归档妥善保存一定期限。对于程远未来签发的证书持有者签名私钥，在其生命周期结束后，无需再保存，可以通过私钥的删除、系统或密码模块的初始化来销毁。

7.5.2.2.11 密码模块的评估

程远未来使用国家密码主管部门批准和许可的密码产品。

7.5.2.3 密钥对管理的其他方面

1、公钥归档

对于生命周期外的CA和证书持有者证书，程远未来将进行归档。归档的证书存放在归档数据库中。

2、证书操作期和密钥对使用期限

证书操作期终止于证书过期或者被撤销。程远未来为证书持有者颁发的证书操作周期通常与密钥对的使用周期是相同的。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。为了保证能够验证在证书有效期内的签名的信息，公钥的使用期限可以在证书的有效期限外。

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。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。

7.5.2.4 激活数据

1、激活数据的产生和安装

存放有程远未来根密钥的加密卡的激活信息（秘密分割），其产生按程远未来密钥生成规程进行。所有秘密分割的创建和分发有相应的记录，包括产生时间、持有人等信息。

程远未来CA私钥的激活数据由硬件加密卡内部产生，并分割保存在5个智能卡中，需通过专门的读卡设备和软件读取。

如果证书持有者证书私钥的激活数据是口令，这些口令必须：

A. 由用户产生；
B. 至少 8 位字符；
C. 至少包含一个字符和一个数字；
D. 至少包含一个小写字母；
E. 不能包含很多相同的字符；
F. 不能和操作员的名字相同；
G. 不能包含用户名信息中的较长的子字符串。

2、激活数据的保护

保存有程远未来CA私钥的激活数据的5个智能卡，由程远未来5个不同的密钥分管员掌管，而且密钥分管员必须符合程远未来职责分割的要求。

如果证书持有者使用口令或 PIN 码保护私钥，证书持有者应妥善保管好其口令或 PIN 码，防止泄露或窃取。

3、激活数据的其他方面

1).激活数据的传送

存有程远未来CA私钥的激活数据的智能卡，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的监督下进行。

当证书持有者证书私钥的激活数据需要进行传送时，证书持有者应保护它们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

2).激活数据的销毁

存有程远未来CA私钥的激活数据的智能卡，其销毁所采取的方法包括将智能卡初始化、或者彻底销毁智能卡，保证不会残留有任何秘密信息。CA私钥激活数据的销毁是在程远未来安全管理人员的监督下进行。

当证书持有者证书私钥的激活数据不需要时应该销毁，证书持有者应该确保无法通过残余信息、介质直接或间接恢复激活数据的部分或全部，比如记录有口令的纸页必须粉碎。

7.5.2.5 计算机安全控制

1、特别的计算机安全技术要求

程远未来系统部署在多级不同厂家的防火墙之内，并进行了安全漏洞扫描和安全优化，安装了防病毒系统，确保了包含CA软件和数据文件的系统是安全可信的系

统，不会受到未经授权的访问，确保系统网络安全。该系统由程远未来系统管理员维护，未经程远未来管理员授权，其它人员不能操作和控制程远未来系统；其它普通证书持有者证书持有者无系统账号和口令。程远未来系统口令有最小口令长度要求，而且必须符合复杂度要求，程远未来系统管理员定期更改系统口令。

7.5.2.6 生命周期技术控制

1、 CA 系统运行管理

程远未来每天由专人负责巡检机房设备的工作情况，定期由运维人员检查软件系统的运行情况。机房部署了漏洞扫描系统、入侵检测系统和防火墙等，以确保网络环境的安全稳定。

A.CA系统的操作流程采用文档化并进行维护。

B.CA系统（包括软件、网络等方面）的变更按系统变更控制流程经管理层批准，经批准的变更实行前通过测试验证，并进行记录。

C.可能对系统的安全性有影响的改动必须事先由管理层得进行风险评估，改动前进行备份并得到管理层的明确批准。

D.CA中心的测试系统、运营系统、网络设施等，都由专门的操作维护人员，并有相应明确的授权。

E.操作维护人员定期检查系统及网络的稳定性、安全性及容量，确定符合服务水平。

F.建立了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。

G.建立了监控流程，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。

H.建立了相应制度，对CA系统相关的媒介（包括设备、证书介质、文档等）进行妥善保管，避免非授权的访问。

2、CA 系统的访问管理

设置关键岗位和职责分工，对于 CA 系统的访问权限进行严格限制，未授权人员不得访问 CA 系统。

A.制定了CA系统的访问策略，内容包括：访问角色及相关权限，认证及鉴别的方法，分权机制，特殊CA操作的人数（密钥生成时3 of 5规则）等。

B.制定了CA系统访问人员角色职能定义，确保合理的职责分割和权限控制，并明确授权及取消授权的操作流程和策略。

C.制定了网络安全策略，并制定了访问网络的控制策略。

D.制定了操作系统及CA软件的安全访问的策略。

E.建立了对各种对CA系统访问的审计措施。

3、 CA 系统的开发和维护

原则上不对 CA 系统进行技术开发和直接调用其数据，仅将 LDAP 和 RA系统对外提供查询和访问服务。

A.建立了CA系统软件修订控制流程，对系统新增或修改进行管理。

B.严格控制对CA系统的源代码及测试数据的访问。

C.操作系统升级变更时，对应用系统软件重新测试。

D.在CA系统中，购买、使用或修改的软件，严格检查，避免“特洛伊木马”等攻击。

7.5.2.7 网络安全控制

程远未来网络中有防火墙、入侵检测、漏洞扫描和网络防病毒等安全机制保护，其配置只允许已授权的机器访问。只有经过授权的程远未来员工才能够进入程远未来签发系统、注册系统、目录服务器、证书发布系统等设备或系统。所有授权用户必须有合法的安全令牌，并且通过密码验证。CA系统只开放与申请证书、查询证书等相关操作功能，其他端口和服务全部关闭。CA系统的边界控制设备拒绝一切非电子认证业务的服务。

7.5.2.8 时间戳

程远未来认证系统的各种系统日志、操作日志有对应的记录时间。这些时间标识未采用基于密码的数字时间戳技术。

第八章 法律责任相关要求

8.1 要求

程远未来在开展电子政务电子认证服务时，按照《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法》等法律法规的要求，对涉及保密、隐私、知识产权、担保以及服务运营等各方面承担相关的责任和义务。

8.2 内容

8.2.1 费用

程远未来通过官网或其他方法通知证书持有者或其他各方费用变化。

8.2.1.1 证书签发和更新费用

根据市场或管理部门的规定决定。

8.2.1.2 证书查询费用

程远未来目前不对证书查询收取专门的费用。

8.2.1.3 证书撤销或状态信息的查询费用

证书撤销列表（CRL）的获取不收取任何费用。程远未来暂未收取OCSP查询服务费，未来根据需要OCSP服务作为增值服务收取费用。

8.2.1.4 其他服务费用

程远未来根据请求者的要求，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。

8.2.1.5 退款策略

如果由于程远未来违背了本证书策略所规定的责任，造成证书持有者合同无法履行、证书持有者证书无法使用，程远未来对证书持有者证书进行撤销并将证书持有者为申请证书所支付的费用退还给证书持有者。

8.2.2 财务责任

程远未来保证具有维持、运作和履行其责任的经济基础，有能力承担对证书持有者、依赖方因合法使用数字证书时而造成的责任风险，并依据本电子政务电子认证服务业务规则规定的方式和范围进行有过错时的赔偿。

8.2.2.1 保险范围

出现下列情形并经公司确认后，证书证书持有者、依赖方等实体可以申请赔偿（法定或约定免责除外）。

1）程远未来在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发，并导致证书持有者或依赖方遭受损失的；

2）程远未来将证书错误的签发给证书持有者以外的第三方，导致证书持有者或者依赖方遭受损失的；

3）由于程远未来的原因导致证书私钥被破译、窃取，导致证书持有者或者依赖方遭受损失的；

4）程远未来未能及时撤销证书，导致证书持有者或者依赖方遭受损失的。

8.2.2.2 其他资产

程远未来目前有能力维护运营和应对可能出现的赔付。

8.2.2.3 对最终实体的保险或担保

程远未来承担证书持有者或依赖方在使用证书过程中造成损失时的举证责任，如无证据证明证书持有者或依赖方使用过程中存在错误操作，则程远未来将按照发布的赔偿办法予以赔偿。

8.2.3 业务信息保密

程远未来有专门的信息保密制度，保护自身和证书持有者的敏感信息、商业秘密。对属于私有信息的业务信息的使用和发布符合法律、法规的要求。

8.2.3.1 业务保密信息范围

程远未来保密的信息包括（但不限于）：

1.证书持有者信息

1) 证书持有者的注册信息；

2) 证书持有者系统、应用访问CRL、OCSP 的记录（时间、频度）；

3) 证书持有者与认证机构、注册机构签订的协议。

2.其他

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证书持有者数字证书以外的信息。

8.2.3.2 不属于保密的信息

程远未来电子政务电子认证服务业务规则、证书申请流程、手续、申请操作指南、证书撤销列表等。

8.2.3.3 保护保密信息的责任

程远未来有各种严格的管理制度、流程和技术手段保护自身的商业秘密，每个员工都必须接受信息保密方面的培训，并与公司签订保密协议。任何参与方有责任保证不泄露保密信息。

8.2.4 个人隐私保密

8.2.4.1 隐私保密方案

程远未来制定有隐私保护制度并签订保密协议，保证证书证书持有者的个人信息不被滥用、未授权使用或出售，同时采取必要措施防止客户资料被遗失、盗用与

篡改。

8.2.4.2 作为隐私处理的信息

作为隐私处理的信息包括：最终证书持有者注册申请证书中提交的信息，包括联系电话、地址等；证书持有者与程远未来、注册机构签订的协议。

8.2.4.3 不被视为隐私的信息

不被认为是隐私信息包括：用来构成证书内容的信息，证书及证书状态。

8.2.4.4 保护隐私的责任

除非执法、司法方面的强制需要，程远未来及其注册机构在没有获得客户授权的情况下，不会将客户隐私信息透露给第三方。

8.2.4.5 使用隐私信息的告知与同意

程远未来或其注册机构如果需要将客户隐私信息用于双方约定的用途以外的目的，则需要事先告知证书持有者并获得证书持有者同意和授权，证书持有者同意和授权信息以下列方式之一传送给程远未来或其注册机构：

1）将手写签名的同意和授权文件邮寄、快递到程远未来或其注册机构；

2）将手写签名的同意和授权文件传真到程远未来或其注册机构；

3）以签名电子邮件的形式同意并授权。

8.2.4.6 依法律或行政程序的信息披露

当程远未来在法律、法规或规章条款有要求时，或在司法机关的要求下必须披露本电子政务电子认证服务业务规则中具有保密性质的信息时，程远未来可以按照法律、法规或规章条款以及司法机关的要求，向执法部门公布相关的保密信息。这种披露不视为违反了保密的要求和义务。

8.2.4.7 其他信息披露情形

对其他信息的披露受制于法律、证书持有者协议。

8.2.5 知识产权

程远未来拥有对本CPS的所有知识产权。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。证书申请者拥有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的可辨识名的所有权利。证书所有者拥有其证书相关的密钥对

的知识产权。

8.2.6 陈述与担保

8.2.6.1 电子认证服务机构的陈述与担保

除非程远未来做出特别约定，若本电子政务电子认证服务业务规则的规定与其他程远未来制定的相关规定、指导方针相互抵触，证书持有者必须接受本电子政务电子认证服务业务规则的约束。在程远未来与包括证书持有者在内的其他方签订的仅约束签约双方的协议中，对协议中未约定的内容，视为双方均同意按本电子政务电子认证服务业务规则的规定执行；对协议中有不同于本电子政务电子认证服务业务规则内容的约定，按双方协议中约定的内容执行。

程远未来承担的责任和义务是：

保证电子认证服务机构本身使用的公钥算法在现有通常技术条件下不会被攻破；保证程远未来的CA签名私钥在程远未来内部得到安全的存放和保护；程远未来建立和执行的安全机制符合国家政策的规定。程远未来不对由于客观意外或其他不可抗力事件造成的操作失败或延迟承担任何损失、损坏或赔偿责任。这些事件包括劳动纠纷、交易一方故意或无意的行为、罢工、暴动、骚动、战争、火灾、爆炸、地震、水灾或其他大灾难等。针对上述内容补充解释如下：

第一：除上述所规定的职责条款，程远未来的服务机构、程远未来注册机构、程远未来的雇员不承担其它任何义务。必须指出，本电子政务电子认证服务业务规则的内容，没有任何信息可以暗示或解释成程远未来必须承担其它的义务或程远未来必须对其行为做出其它的承诺。

第二：在上述内容中所罗列不可抗力的任何情况下，程远未来由于受到影响，可免除本节所述的责任和相应的证书策略规定的责任和义务。

第三：由于技术的进步与发展，为保证证书的安全性，程远未来会要求证书持有者及时更换证书以保证程远未来能更好地履行本节所述之责任。

8.2.6.2 注册机构的陈述与担保

注册机构必须遵守所有的登记程序和安全保障措施。这些程序和保障由程远未来决定，并在本电子政务电子认证服务业务规则或相应的注册机构协议中规定，以后程远未来可以根据情况修改有关内容，并及时公布。注册机构必须遵守和符合本电子政务电子认证服务业务规则的条款。

8.2.6.3 证书持有者的陈述与担保

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

证书持有者在证书申请表上填列的所有声明和信息必须是完整、真实和准确的，可供程远未来或受理点检查和核实；

证书持有者必须严格遵守和服从电子政务电子认证服务业务规则规定的以及由程远未来推荐使用的安全措施；

证书持有者需熟悉本电子政务电子认证服务业务规则的内容和要求与证书相关的证书政策，遵守证书持有者证书使用方面的有关限制；

一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘或泄密以及其他情况，证书持有者应立刻通知程远未来或程远未来注册机构，申请采取挂失、废除等处理措施。

8.2.6.4 依赖方的陈述与担保

依赖方确认，在任何信赖行为发生之前，阅读了依赖方协议，并评估了在特定应用中信赖证书的适当性，不在证书适用目的以外的应用中信任证书。依赖方在信赖证书前，对证书的信任链进行验证，并通过查询CRL或OCSP确认证书是否被撤销。

8.2.6.5 其他参与者的陈述与担保

遵守本CPS的所有规定。

8.2.7 担保免责

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。

8.2.8 有限责任

证书持有者、依赖方因程远未来提供的电子认证服务从事民事活动遭受损失，程远未来将承担不超过本CPS 8.2.9规定的有限赔偿责任。

8.2.9 赔偿

1）对于由如下原因造成的证书持有者或依赖方损失，程远未来对证书持有者或依赖方进行赔偿：

（1）程远未来在批准证书前没有严格按业务程序确认证书申请，造成证书的错

误签发，并导致用户或依赖方遭受损失的；

（2）程远未来将证书错误的签发给用户以外的第三方，导致用户或者依赖方遭受损失的。

2）在如下情况，证书持有者对自身原因造成的程远未来、依赖方损失承担责任：

（1）证书持有者在证书申请中对事实的虚假或错误描述；

（2）在证书申请中证书持有者没有披露与申请证书相关的重要的事实，如果这种错误表述或遗漏是因为粗心或故意欺骗任何一方；

（3）证书持有者没有使用可信系统保护私钥，或者没有采取必要的注意防止证书持有者私钥的安全损害、丢失、泄漏、修改或非授权的使用；

（4）证书持有者使用的名字（包括但不限于通用名、域名和e-mail 地址）侵犯了第三方的知识产权。

3）在如下情况，依赖方对自身原因造成程远未来损失承担责任：

（1）依赖方没有执行依赖方职责义务；

（2）在不合理的环境下信赖一个证书，如依赖方明知证书存在超范围、超期限使用的情形或证书已经或有可能被人窃取的情形，但仍然信赖证书；

（3）依赖方没有检查证书状态，没有确定证书是否过期或撤销。

4）程远未来承担赔偿责任（法定或约定免责除外）的赔偿限制如下：

（1）程远未来对任何证书证书持有者、依赖方等实体有关证书赔偿的合计赔偿上限可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。

（2）对于由证书持有者或依赖方的原因造成的损失，程远未来不承担责任，由证书持有者 或依赖方自行承担。

（3）程远未来只有在其证书有效期限内承担损失损害赔偿。

8.2.10 有效期限与终止

8.2.10.1 有效期限

本CPS自发布之日起生效。

8.2.10.2 终止

当新版本的CPS生效时或程远未来终止业务时，旧版本CPS自动终止；当程远未来中止业务时，程远未来CPS自动终止。

8.2.10.3 效力的终止与保留

本CPS终止后，已签发符合本证书策略的证书，效力作用直到证书到期或撤消。当由于某种原因，如内容修改、与适用法律相冲突，证书策略、电子政务电子认证服务业务规则、证书持有者协议、依赖方协议和其他协议中的某些条款失效后，不影响文件中其他条款的法律效力。

8.2.11 对参与者的个别通告与沟通

程远未来及其注册机构在必要的情况下，如在主动撤销证书持有者证书、发现证书持有者将证书用于规定外用途及证书持有者其他违反证书持有者协议的行为时，会通过适当方式，如电话、电邮、信函、传真等，个别通知证书持有者、依赖方。

8.2.12 修订

程远未来有权在合适的时间修订本电子政务电子认证服务业务规则中任何术语、条件和条款，而且无须预先通知任何一方。

程远未来有权在官方网站中公布修改结果。所有的修订在公布后立刻生效。

8.2.12.1 修订程序

CPS中所列条款不能适应运营的实际需求，或者与现行法律相抵触时，程远未来有权在合适的时间修订本CPS中任何术语、条件和条款，而且无须预先通知任何一方。

本CPS的修订，由程远未来CPS起草小组组织讨论，提出修订报告，报程远未来安全策略委员会批准后，由CPS起草小组组织修订，修订后的CPS经过程远未来安全策略委员会审查通过后正式实施并报国家密码管理局备案。

8.2.12.2 通知机制和期限

修改后的CPS经批准后将立即在程远未来网站更新发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，程远未来将在合理的时间内通知有关各方，合理的时间保证有关方面受到的影响最小。

程远未来保留随时对CPS进行修订的权利，进行下列（但不限于）不重要的修订后将不作通知：对印刷错误的更正、URL的改变和联系人信息的变更等。

8.2.12.3 必须修改业务规则的情形

由程远未来安全中心根据公司业务情况提出，程远未来安全管理委员会审批。

8.2.13 争议处理

如果各参与方之间无法协商解决出现的问题和争端，可通过法律途径解决。

8.2.14 管辖法律

本规则在各方面服从《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法》等中华人民共和国法律、规则、规章、法令和政令的约束和解释。程远未来的任何业务活动受有关法律、法规的制约，任何业务和法律文件、合同的解释、执行不能同有关法律、法规相冲突。

8.2.15 与适用法律的符合性

本CPS的使用也必须遵从使用地的相关法律和法规。

8.2.16 一般条款

8.2.16.1 完整协议

CP、CPS、证书持有者协议及依赖方协议及其补充协议将构成程远未来信任域参与者间的完整协议。

8.2.16.2 转让

程远未来、注册机构、证书持有者及依赖方之间的责任、义务不能通过任何形式转让给其他方。

8.2.16.3 分割性

法律允许的范围内，在程远未来证书持有者协议、依赖方协议和其他证书持有者协议内出现可以同其他条款分割的条款时，协议中的可分割条款的无效不应该影响协议中其 他条款效力。

8.2.16.4 强制执行力

在程远未来、注册机构、证书持有者和依赖方之间出现纠纷、诉讼时，胜诉可以要求对方支付有关诉讼费作为对其补偿的一部分。免除一方对某次合同违约的赔偿，不意味着免除对其他合同违约的赔偿。

8.2.16.5 不可抗力

当由于不可抗力，如地震、洪灾、雷电等自然灾害和战争等，造成程远未来、注册机构无法提供正常的服务时，程远未来、注册机构不承担由此给客户造成的损失。

8.2.17 其他条款

程远未来对本CPS具有最终解释权。