

FJCA

电子认证业务规则

版本 2.1



发布日期：2009 年 2月 1日

生效日期：2009 年 3月 1日

福建省数字安全证书管理有限公司

Copyright © Fujian Digital Certificate Authority CO.,Ltd.

版权声明

福建省数字安全证书管理有限公司（简称 FJCA），完全拥有本文件的版权。本文件所涉及的“FJCA”及其图标等是由福建省数字安全证书管理有限公司独立持有的，受到完全的版权保护。

未经福建省数字安全证书管理有限公司的书面同意，本文件的任何部分不得以任何方式、任何途径（包括但不限于电子的、机械的、影印、录制）进行部分的转载、粘贴或发布本文件，更不得更改本文件的部分词汇进行转贴。

福建省数字安全证书管理有限公司拥有对本电子认证业务规则的最终解释权。

对任何复制本文件的其他请求，请寄往以下地址：

单 位：福建省数字安全证书管理有限公司

地 址：福建省福州市温泉公园路188号

邮政编码：350003

联系电话：0591-968806

传 真：0591-87816483

电子邮件：CPS@fjca.com.cn

修订表

版本	日期	备注
1.0	2002年1月26日	根据《福建省电子商务证书认证中心对外运营策略和规范》和《RFC》相关标准编写电子认证规则。
1.2	2004年5月31日	根据实际应用发展情况修改。
2.0	2005年12月9日	根据《中华人民共和国电子签名》《电子认证服务管理办法》和中华人民共和国信息产业部颁布的《电子认证规则（试行）完全版》进行修改。
2.1	2009年2月1日	根据中华人民共和国工业和信息化部 2007 年度审意见修改。

目 录

1. 概括性描述	10
1.1 概述.....	10
1.2 文档名称与标识.....	10
1.3 电子认证活动参与者.....	10
1.3.1 电子认证服务机构	10
1.3.2 注册机构.....	11
1.3.3 订户	11
1.3.4 依赖方.....	11
1.3.5 其他参与者	11
1.4 证书应用	11
1.4.1 适合的证书应用	11
1.4.2 限制的证书应用	12
1.5 策略管理	12
1.5.1 策略文档管理机构	12
1.5.2 联系人.....	12
1.5.3 决定 CPS 符合策略的机构.....	13
1.5.4 CPS 批准程序	13
1.6 定义和缩写	13
2. 信息发布与信息管理.....	14
2.1 认证信息的发布.....	14
2.2 发布时间或频率.....	15
2.3 信息库访问控制.....	15
3. 身份标识与鉴别	15
3.1 命名.....	15
3.1.1 名称类型.....	15
3.1.2 对名称意义化的要求.....	16
3.1.3 订户的匿名或伪名	16
3.1.4 理解不同名称形式的规则.....	16
3.1.5 名称的唯一性	16
3.1.6 商标的识别、鉴别和角色.....	16
3.2 初始身份确认.....	16
3.2.1 证明拥有私钥的方法.....	16
3.2.2 组织机构身份的鉴别.....	17
3.2.3 个人身份的鉴别	18
3.2.4 没有验证的订户信息.....	18
3.2.5 授权确认.....	18
3.2.6 互操作准则.....	19

3.3 密钥更新请求的标识与鉴别	19
3.3.1 常规密钥更新的标识与鉴别	19
3.3.2 吊销后密钥更新的标识与鉴别	19
3.4 吊销请求的标识与鉴别	19
4. 证书生命周期操作要求.....	20
4.1 证书申请	20
4.1.1 证书申请实体	20
4.1.2 证书申请过程与责任	20
4.2 证书申请处理.....	20
4.2.1 执行识别与鉴别功能.....	20
4.2.2 证书申请批准和拒绝.....	20
4.2.3 处理证书申请的时间.....	21
4.3 证书签发	21
4.3.1 证书签发过程中电子认证服务机构的行为	21
4.3.2 电子认证服务机构对订户的通告	21
4.4 证书发布	22
4.4.1 电子认证服务机构对证书的发布	22
4.4.2 电子认证服务机构对其他实体的通告	22
4.5 密钥对和证书的使用	22
4.5.1 订户私钥和证书的使用	22
4.5.2 依赖方对公钥和证书的使用	22
4.6 证书更新	23
4.6.1 证书更新的情形	23
4.6.2 请求证书更新的实体.....	23
4.6.3 证书更新请求的处理.....	23
4.6.4 颁发新证书时对订户的通告	24
4.6.5 构成接受更新证书的行为	24
4.6.6 电子认证服务机构对更新证书的发布.....	24
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.....	24
4.7 证书密钥更新.....	25
4.7.1 证书密钥更新的情形.....	25
4.7.2 请求证书密钥更新的实体.....	25
4.7.3 证书密钥更新请求的处理.....	25
4.7.4 颁发新证书对订户的通告	25
4.7.5 构成接受密钥更新证书的行为	26
4.7.6 电子认证服务机构对密钥更新证书的发布	26
4.7.7 电子认证服务机构对其他实体的通告.....	26
4.8 证书变更	26
4.8.1 证书变更的情形	26
4.8.2 请求证书变更的实体.....	26
4.8.3 证书变更请求的处理.....	26
4.8.4 颁发新证书时对订户的通告	27
4.8.5 构成接受变更证书的行为	27

4.8.6	电子认证服务机构对变更证书的发布	27
4.8.7	电子认证服务机构对其他实体的通告	27
4.9	证书吊销和挂起	28
4.9.1	证书吊销的情形	28
4.9.2	请求证书吊销的实体	28
4.9.3	吊销请求的流程	28
4.9.4	吊销请求宽限期	29
4.9.5	电子认证服务机构处理吊销请求的时限	29
4.9.6	依赖方检查证书吊销的要求	29
4.9.7	CRL 的颁发频率	30
4.9.8	CRL 发布的最大滞后时间	30
4.10	证书状态服务	30
4.10.1	操作特点	30
4.10.2	服务可用性	30
4.10.3	可选特征	30
4.11	订购结束	30
4.12	密钥生成、备份与恢复	31
4.12.1	密钥生成、备份与恢复的策略和行为	31
4.12.2	会话密钥的封装与恢复的策略和行为	31
5.	电子电子认证服务机构设施、管理和操作控制	32
5.1	物理控制	32
5.1.1	场地位置与建筑	32
5.1.2	物理访问	32
5.1.3	电力与空调	33
5.1.4	水患防治	33
5.1.5	火灾防护	34
5.1.6	介质存储	35
5.1.7	废物处理	35
5.1.8	异地备份	35
5.2	程序控制	35
5.2.1	可信角色	35
5.2.2	每项任务需要的人数	37
5.2.3	每个角色的识别与鉴别	37
5.2.4	需要职责分割的角色	38
5.3	人员控制	38
5.3.1	资格、经历和无过失要求	38
5.3.2	背景审查程序	38
5.3.3	培训要求	39
5.3.4	再培训周期和要求	39
5.3.5	工作岗位轮换周期和顺序	39
5.3.6	对未授权行为的处罚	40
5.3.7	独立合约人的要求	40
5.3.8	提供给员工的文档	40

5.4 审计日志程序.....	40
5.4.1 记录事件的类型	40
5.4.2 处理日志的周期	41
5.4.3 审计日志的保存期限.....	41
5.4.4 审计日志的保护	41
5.4.5 审计日志备份程序	41
5.4.6 审计日志收集系统	41
5.4.7 对导致事件实体的通告.....	42
5.4.8 脆弱性评估	42
5.5 记录归档	42
5.5.1 归档记录的类型	42
5.5.2 归档记录的保存期限.....	42
5.5.3 归档文件的保护	43
5.5.4 归档文件的备份程序.....	43
5.5.5 记录时间戳要求	43
5.5.6 获得和检验归档信息的程序.....	44
5.6 电子认证服务机构密钥更替.....	44
5.7 损害和灾难恢复.....	44
5.7.1 事故和损害处理程序.....	44
5.7.2 计算资源、软件和/或数据的损坏	45
5.7.3 实体私钥损害处理程序.....	45
5.7.4 灾难后的业务连续性能力.....	46
5.8 电子认证服务机构或注册机构的终止.....	46
6. 认证系统技术安全控制.....	47
6.1 密钥对的生成和安装.....	47
6.1.1 密钥对的生成	47
6.1.2 私钥传送给订户	47
6.1.3 公钥传送给证书签发机构.....	47
6.1.4 电子认证服务机构公钥传送给依赖方.....	47
6.1.5 密钥的长度	47
6.1.6 公钥参数的生成和质量检查	48
6.1.7 密钥使用目的	48
6.2 私钥保护和密码模块工程控制.....	48
6.2.1 密码模块标准和控制.....	48
6.2.2 私钥的多人控制	48
6.2.3 私钥托管	49
6.2.4 私钥备份	49
6.2.5 私钥归档.....	49
6.2.6 私钥导入、导出密码模块.....	49
6.2.7 私钥在密码模块中的存储.....	49
6.2.8 激活私钥的方法	49
6.2.9 解除私钥激活状态的方法.....	50
6.2.10 销毁密钥的方法	50

6.2.11 密码模块的评估	50
6.3 密钥对管理的其他方面	50
6.3.1 公钥归档	50
6.3.2 证书操作期和密钥对使用期限	51
6.4 激活数据	51
6.4.1 激活数据的产生和安装	51
6.4.2 激活数据的保护	51
6.4.3 激活数据的其他方面	51
6.5 计算机安全控制	51
6.5.1 特别的计算机安全技术要求	51
6.5.2 计算机安全评估	52
6.6 生命周期技术控制	52
6.6.1 系统开发控制	52
6.6.2 安全管理控制	52
6.6.3 生命周期的安全控制	52
6.7 网络的安全控制	53
6.8 时间戳	53
7. 证书、证书吊销列表和在线证书状态协议	53
7.1 证书	53
7.1.1 版本号	53
7.1.2 证书扩展项	53
7.1.3 算法对象标识符	54
7.1.4 名称形式	54
7.2 证书吊销列表	55
7.2.1 版本号	55
7.2.2 CRL 和 CRL 条目扩展项	55
7.3 在线证书状态协议	55
7.3.1 版本号	55
7.3.2 OCSP 扩展项	56
8. 电子认证服务机构审计和其他评估	56
8.1 评估的频率或情形	56
8.2 评估者的资质	56
8.3 评估者与被评估者之间的关系	57
8.4 评估内容	57
8.5 对问题与不足采取的措施	57
8.6 评估结果的传达与发布	58
9. 法律责任和其他业务条款	58
9.1 费用	58
9.1.1 证书签发和更新费用	58
9.1.2 证书查询费用	58

9.1.3 证书吊销或状态信息的查询费用	58
9.1.4 其他服务的费用	58
9.1.5 退款策略	59
9.2 财务责任	59
9.3 业务信息保密	59
9.3.1 保密信息范围	59
9.3.2 不属于保密的信息	60
9.3.3 保护保密信息的信息	60
9.4 个人隐私保密	60
9.4.1 隐私保密方案	60
9.4.2 作为隐私处理的信息	60
9.4.3 不被视为隐私的信息	61
9.4.4 保护隐私的责任	61
9.4.5 使用隐私信息的告知或同意	61
9.4.6 依法律或行政程序的信息披露	61
9.4.7 其他信息披露情形	61
9.5 知识产权	61
9.6 陈述与担保	62
9.6.1 电子认证服务机构的陈述与担保	62
9.6.2 注册机构的陈述与担保	62
9.6.3 订户的陈述与担保	63
9.6.4 依赖方的陈述与担保	63
9.6.5 其他参与者的陈述与担保	63
9.7 赔偿与担保免责	64
9.7.1 用户申请 FJCA 赔偿	64
9.7.2 FJCA 申请用户赔偿	64
9.7.3 赔偿限额	65
9.7.4 责任免除	65
9.8 有效期限与终止	66
9.8.1 有效期限	66
9.8.2 终止	66
9.8.3 效力的终止与保留	66
9.9 对参与者的个别通告与沟通	66
9.10 修订	67
9.10.1 修订程序	67
9.10.2 通告机制和期限	67
9.10.3 必须修改业务规则的情形	67
9.11 争议处理	67
9.12 管辖法律	68
9.13 与适用法律的符合性	68
9.14 一般条款	68
9.14.1 完整协议	68
9.14.2 分割性	68
9.14.3 强制执行	68

9.14.4 不可抗力.....	68
9.15 其他条款.....	69

1. 概括性描述

1.1 概述

FJCA 电子认证业务规则（以下简称《电子认证业务规则》）由福建省数字安全证书管理有限公司按照中华人民共和国工业和信息化部《电子认证服务管理办法》的要求，依据《电子认证业务规则规范(试行)》制定，并报中华人民共和国工业和信息化部备案。

福建省数字安全证书管理有限公司（Fujian Digital Certificate Authority CO.,Ltd.，简称 FJCA）于 2001 年 10 月开始运营，是权威、公正的电子认证服务机构。FJCA 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，为电子政务、电子商务、企业信息化构建安全、可靠的信任环境。

本《电子认证业务规则》详细阐述了 FJCA 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 FJCA 及其员工、注册机构、证书申请人、订户和依赖方，各参与方必须完整地理解和执行本《电子认证业务规则》所规定的条款，并承担相应的责任和业务。

1.2 文档名称与标识

文档名称是《FJCA 电子认证业务规则》，目前版本号为 V2.1，在 FJCA 运营网站发布，网站地址为 www.fjca.com.cn

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

FJCA 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。

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。

1.3.2 注册机构

注册机构作为电子认证服务机构授权委托的下属机构，包括注册系统（RA 系统）和证书本地受理点，负责受理证书申请。

1.3.3 订户

订户是从 FJCA 接收数字证书的实体。在电子签名应用中，订户即为电子签名人。

1.3.4 依赖方

依赖方是依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。在 FJCA 证书服务体系中，是信任 FJCA 证书，可以对使用 FJCA 证书机制进行的数字签名进行验证，使用其他 FJCA 证书的公钥的实体。

1.3.5 其他参与者

其他参与者指为 FJCA 证书服务体系提供相关服务的其他实体。

1.4 证书应用

1.4.1 适合的证书应用

FJCA 证书目前已经在电子商务、电子政务、企业信息化、网上信息传递、网上银行等多领域应用，为建设网络信任环境提供了基础性的信任服务。详细信息请参阅 <http://www.fjca.com.cn>。证书申请、订户和依赖方等各类主体可以根据实际需要，自主判断和决定采用相应合适的证书类型，以及了解证书的应用类型、

应用范围，选择自己的应用方式，详情请咨询 0591-968806。

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和使用于 FJCA 不认可的证书应用系统，否则由此造成的法律后果由订户承担。

1.5 策略管理

1.5.1 策略文档管理机构

根据中华人民共和国电子签名法、中华人民共和国工业和信息化部（原信息产业部）电子认证服务管理办法和电子认证业务规则规范的要求，FJCA 制定本《电子认证业务规则》，并指定专门的机构---FJCA 运营安全管理小组。

本《电子认证业务规则》的制订、发布、更新等事宜，由 FJCA 设立“CPS 编写小组”，CPS 编写小组具体为行政部、运行部、技术开发部、客户服务部、制证部、市场部等派人参加。

本《电子认证业务规则》由福建省数字安全证书管理有限公司拥有完全版权。

1.5.2 联系人

本《电子认证业务规则》在 FJCA 网站发布，对具体个人不另行通知。

网站地址：<http://www.fjca.com.cn>

电子邮箱：cps@fjca.com.cn

联系地址：福建省福州市温泉公园路 188 号

邮 编：350003

电话号码：0591-87873460

传真号码：0591-87856110

1.5.3 决定 CPS 符合策略的机构

本《电子认证业务规则》由 FJCA 运营安全管理小组制定并执行。

1.5.4 CPS 批准程序

“CPS 编写小组”负责起草和修订 CPS 形成讨论稿（或 CPS 修订内容），并征求意见，经讨论、修改达成一致意见形成送审稿。具体流程如下：

“CPS编写小组”负责将CPS送审稿提交法律顾问审阅。在取得法律顾问针对相关法律问题的审查意见后，“CPS编写小组”提交FJCA运营安全管理小组，并组织对CPS草案进行评审。在评审过程中，可提出修改意见，由“CPS编写小组”进行修改。评审通过后在FJCA网站上对外公布。从对外公布之日起三十个工作日内向中华人民共和国工业和信息化部备案。

注：法律意见——对外公布及备案的流程应严格遵守中华人民共和国工业和信息化部的相关规定。

1.6 定义和缩写

下列定义适用于本《电子认证业务规则》：

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

支持公开密钥体制的安全基础设施，提供身份鉴别、加密、完整性和不可否认性服务。

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

关于证书电子认证服务机构在签发、管理、吊销或更新证书(或更新证书中的密钥)过程中所采纳的业务实践的声明。

c) 电子认证服务机构（CA）Certification Authority

受用户信任，负责创建和分配公钥证书的权威机构。

d) 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（即 RA 代表

CA 承担某些任务)。

e) 电子签名认证证书(证书)Digital Certificate

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

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

一个经电子认证服务机构数字签名的列表，它指定了一系列证书颁发者认为无效的证书，也称黑名单服务。

g) CA 注销列表(ARL): Certificate 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。

h) 私钥(电子签名制作数据) Private Key

指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。

私钥是经由数字运算产生的密钥，用于制作电子签名数据，亦可依据其运算方式，就相对应的公开密钥加密的文件或信息予以解密。

i) 公钥(电子签名验证数据) Public Key

公钥是经由数字运算产生的密钥，用于解密电子签名，确认电子签名人的身份及电子签名的真实性。

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

电子签名验证数据是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。如果电子签名制作数据表现为私钥，则电子签名验证数据就是公钥。

2. 信息发布与信息管理

2.1 认证信息的发布

FJCA 通过网站公布以下信息：《电子认证业务规则》修订以及其他由 FJCA

不定时发出的信息。FJCA 网址：<http://www.fjca.com.cn>。

本《电子认证业务规则》发布在 FJCA 的网站上，供相关方下载、查阅。FJCA 通过目录服务器发布订户的证书和 CRL，订户或信赖方可以通过访问 FJCA 的目录服务器获取证书的信息和吊销证书列表。同时，FJCA 提供在线证书状态查询服务。

2.2 发布时间或频率

- a) 《电子认证业务规则》一经网站发布，即时生效。对数字证书的订户及证书申请人均具备约束力。对具体个人不另行通知。
- b) 证书的发布：在证书签发时，FJCA 通过目录服务器自动将该证书公布。
- c) FJCA 的 CRL 每 1 小时发布一次。

2.3 信息库访问控制

对于公开发布的 CPS、证书、CRL 等公开信息，FJCA 允许公众自行通过网站和目录服务器进行查询和访问。

只有经授权的 RA/CA 管理员可以查询电子认证服务机构和注册机构数据库中的其他数据。

3. 身份标识与鉴别

3.1 命名

3.1.1 名称类型

每个订户对应一个甄别名（Distinguished Name，简称 DN）。

数字证书中的主体的 X.500 DN 是 C=CN 命名空间下的 X.500 目录唯一名字。

3.1.2 对名称意义化的要求

订户的甄别名(DN)必须具有一定的代表意义。

证书主体名称标识本证书所提到的最终实体的特定名称，描述了与主体公钥中的公钥绑定的实体信息。

3.1.3 订户的匿名或伪名

在 FJCA 证书服务体系中，订户(证书申请人)不得使用匿名或伪名。

3.1.4 理解不同名称形式的规则

DN 的具体内容依次由 CN、OU、O、L、S、C 六部分组成。其中 CN 用来表示用户名，OU、O 用来表示组织单位名称、L 用来表示地址、S 用来表示省、C 用来表示国家。

3.1.5 名称的唯一性

在 FJCA 证书服务体系中，证书主体名称必须是唯一的。

3.1.6 商标的识别、鉴别和角色

本《电子认证业务规则》受到完全的版权保护，本文件中涉及的“FJCA”及其图标等是由福建省数字安全证书管理有限公司独立持有的专有商标。其他参与者的商标为其拥有方所有。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

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。在 FJCA 证书服务体系中，私钥在用户端生成，证书请求信息中包含用

私钥进行的数字签名，CA 用其对应的公钥来验证这个签名。

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

3.2.2 组织机构身份的鉴别

对于组织机构身份的鉴别，FJCA 需要验证组织机构的合法证件。证书申请人需持工商营业执照或全国组织机构代码证书等证件，以及组织机构给经办人的授权和经办人身份证件，向 CA 机构提出申请。如该企业需申请服务器类型的证书，还需向注册机构提交域名证明文件。

组织机构身份的鉴别规范简要说明了如何进行组织机构身份鉴别。FJCA 保留根据最新国家政策法规的要求更新组织机构身份鉴别规范的权利。更新后的组织机构身份鉴别规范将发布在 FJCA 的网站上：<http://www.fjca.com.cn>。

经办人经组织授权，并携带组织机构授权给经办人申请办理证书事宜的授权文件及本人身份证的原件和复印件，到 FJCA 授权的注册机构提交书面数字证书申请表(一式两份)及下述组织机构证明文件等申请资料，并缴纳证书服务费用。

a) 组织机构代码证的副本及复印件；

b) 法人营业执照副本及复印件，如果组织机构没有营业执照，则书面申请表上可选其他有效证件的副本及复印件，部分有效证件如下：

- 1) 企业法人营业执照
- 2) 事业单位法人登记证
- 3) 事业单位登记证
- 4) 社会团体登记证
- 5) 地税税务登记证
- 6) 政府批文
- 7) 其他有效证件

c) 经办人有效身份证件的原件和复印件；

d) 如该组织机构需申请服务器类型的证书，还需向注册机构提交域名使用权证明材料。

(注：以上 a)、b)和 d)证明文件的复印件需加盖申请单位公章)。

FJCA 授权的注册机构按照 FJCA 组织机构身份鉴别规范对申请资料的原件和复印件真实性进行审核，并进行批准申请或拒绝申请的操作。

批准申请后 FJCA 或注册机构将保留相关盖单位公章的证明材料复印件，与证书申请表一并存档保存。

3.2.3 个人身份的鉴别

个人身份的鉴别可以使用以下有效的身份证件：港澳台居民身份证、户口簿、护照、军官证、警官证、外国人永久居留证、士兵证、身份证、士官证和文职干部证。

个人身份的鉴别规范简要说明了如何进行个人身份鉴别。FJCA 保留根据最新政策法规的要求更新个人身份鉴别规范的权利。更新后的个人身份鉴别规范将发布在 FJCA 的网站上：<http://www.fjca.com.cn>。

个人需持上述个人有效身份证件，到 FJCA 授权的注册机构提交书面数字证书申请表(一式两份)和上述有效身份证件的复印件等申请资料，并缴纳证书服务费用。

FJCA 授权的注册机构按照 FJCA 个人身份鉴别规范对申请资料的原件和复印件真实性进行审核，并进行批准申请或拒绝申请的操作。

批准申请后，FJCA 或注册机构将保留复印件，与证书申请表一并存档保存。

3.2.4 没有验证的订户信息

订户提交鉴证文件以外的信息为没有验证的订户信息。

3.2.5 授权确认

为确保办理人具有特定的许可，代表组织机构获取数字证书，需要出具组织机构授权 其该组织机构为办理 FJCA 数字证书事宜的授权文件。

组织机构在 FJCA 的数字证书申请表上加盖单位公章后，则证明本组织机构

对办理人的授权确认。

3.2.6 互操作准则

不在此规定。

3.3 密钥更新请求的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

在常规密钥更新中，通过订户使用当前有效私钥对包含新公钥的密钥更新请求进行签名，FJCA 使用订户原有公钥验证确认签名来进行订户身份标识和鉴别。

3.3.2 吊销后密钥更新的标识与鉴别

吊销后密钥更新中对身份标识和鉴别的要求，使用原始身份验证相同的流程，详见 § 3.2.2 组织机构身份的鉴别和 3.2.3 个人身份的鉴别。

3.4 吊销请求的标识与鉴别

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

如果是因为订户没有履行本《电子认证业务规则》所规定的义务，由注册机构申请吊销订户的证书时，不需要对订户身份进行标识和鉴别。

4. 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

证书申请实体包括个人和具有独立法人资格的组织机构(包括行政机关、事业单位、企业单位、社会团体和人民团体等)。

4.1.2 证书申请过程与责任

证书申请人按照本《电子认证服务规则》所规定的要求,填写证书申请表,并准备相关的身份证明材料。FJCA 或注册机构依据身份鉴别规范对证书申请人的身份进行鉴别,并决定是否受理申请。

申请过程中各方责任为:订户要按照本《电子认证服务规则》的要求准备证书申请材料,并确保申请材料真实准确。

注册机构负责接收证书申请人的请求材料,当面对订户所提供的证书申请信息与身份证明资料的一致性进行查验。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

FJCA 或授权的注册机构按照本《电子认证业务规则》所规定的身份鉴别流程对申请人的身份进行识别与鉴别。具体的鉴别流程详见 § 3.2.2 组织机构身份的鉴别和 3.2.3 个人身份的鉴别。

4.2.2 证书申请批准和拒绝

FJCA 或授权的注册机构根据本《电子认证业务规则》所规定的身份鉴别流程对证书申请人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。

如果证书申请人通过本《电子认证业务规则》所规定的身份鉴别流程且鉴证结果为合格，FJCA 或注册机构将批准证书申请，为证书申请人制作并颁发数字证书。

证书申请人未能通过身份鉴证，FJCA 或注册机构将拒绝申请人的证书申请，并通知申请人鉴证失败，同时向申请人提供失败的原因(法律禁止的除外)。

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

4.2.3 处理证书申请的时间

FJCA 授权的注册机构尽快确认证书申请信息，一旦注册机构收到了所有必须的相关信息，将在 24 小时内处理证书申请。

注册机构能否在上述时间期限内处理证书申请取决于证书申请人是否真实、完整、准确地提交了相关信息和是否及时地响应了 FJCA 的管理要求。

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

FJCA 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，FJCA 所签发的证书在 24 小时后才生效。

4.3.2 电子认证服务机构对订户的通告

电子认证服务机构通过注册机构，对订户的通告有以下几种方式：

a) 通过面对面的方式，通知订户到注册机构领取数字证书；注册机构把密码信封和证书等直接提交给订户，通知订户证书信息已经正确生成；

b) 其他 FJCA 认为安全可行的方式通知订户。

4.4 证书发布

4.4.1 电子认证服务机构对证书的发布

FJCA 在签发完证书后，就将证书发布到数据库和目录服务器中。

FJCA 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写入主目录服务器中，然后通过主从映射，将主目录服务器的数据自动发布到从目录服务器中，供订户和依赖方查询和下载。

4.4.2 电子认证服务机构对其他实体的通告

其他实体可以通过从目录服务器中查询到 FJCA 已经签发的数字证书。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户在提交了证书申请并接受了 FJCA 所签发的证书后，均视为已经同意遵守与 FJCA、依赖方有关的权利和义务的条款。订户接受到数字证书，应妥善保存其证书对应的私钥。

订户只能在指定的应用范围内使用私钥和证书，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吊销之后，订户必须停止使用该证书对应的私钥。

4.5.2 依赖方对公钥和证书的使用

依赖方只能在恰当的应用范围内依赖于证书，并且与证书要求相一致（如密钥用途扩展等）。依赖方获得对方的证书和公钥后，可以通过查看对方的证书了解对方的身份，并通过公钥验证对方电子签名的真实性。验证证书的有效性包括三个方面的内容：

a) 用 FJCA 的证书验证证书中的签名，确认该证书是 FJCA 签发的，并且

证书的内容没有被篡改。

- b) 检验证书的有效期，确认该证书在有效期之内。
- c) 查询证书状态，确认该证书没有被注销。

在验证电子签名时，依赖方应准确知道什么数据已被签名。在公钥密码标准里，标准的签名信息格式被用来准确表示签名过的数据。

4.6 证书更新

4.6.1 证书更新的情形

证书更新是指在不改变证书中订户的公钥或其他任何信息的情况下，为订户签发一张新证书。

在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至日期。订户应当在证书有效期到期前，到 FJCA 授权的注册机构申请更新证书。

证书更新的具体情形如下：

- a) 证书的有效期将要到期；
- b) 密钥对的使用期将要到期；
- c) 因私钥泄漏而吊销证书后，就需要进行证书更新；
- d) 其他。

4.6.2 请求证书更新的实体

订户可以请求证书更新。订户包括持有 FJCA 签发的个人、组织及设备等各类证书的证书持有人。

4.6.3 证书更新请求的处理

处理证书更新请求可以采用两种方式：一种方式是在线自动更新。对于证书信息无须改变的订户，在证书即将过期时，在获得 FJCA 授权后，自助进行在线证书更新操作，获得新证书。

另一种方式是人工方式更新。对于证书信息发生改变的订户，由注册机构

来处理证书更新请求，为订户制作新的证书。

注册机构对申请证书更新订户的进行查验与鉴别，鉴别要求同本《电子认证业务规则》3.2.2 和 3.2.3。

4.6.4 颁发新证书时对订户的通告

在线自动更新方式，在自动完成更新，给订户颁发新证书时，在线更新系统会自动通知证书更新已完成，新证书已颁发。

人工更新方式，对订户的通告有以下几种方式：

- a) 通过面对面的方式，通知证书更新已完成，新证书已颁发；
- b) 邮政信函通知订户；
- c) 其他 FJCA 认为安全可行的方式通知订户。

4.6.5 构成接受更新证书的行为

在线更新方式，当订户对在线系统提示证书更新已完成，新证书已颁发进行确认时，就表示订户接受更新证书。

人工更新方式，当更新证书签发后，注册机构将证书及其密码信封当面或寄送给订户，就表示订户接受更新证书。

4.6.6 电子认证服务机构对更新证书的发布

FJCA 在签发更新证书后，就将更新证书发布到数据库和目录服务器中，对外进行发布。

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

其他实体可以通过从目录服务器中查询已更新的数字证书。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

- a) 证书的有效期将要到期，证书更新；
- b) 因私钥泄漏而吊销证书；
- c) 其他。

4.7.2 请求证书密钥更新的实体

订户可以请求证书密钥更新。订户包括持有 FJCA 签发的个人、组织及设备等各类证书的证书持有人。

4.7.3 证书密钥更新请求的处理

处理证书密钥更新请求可以采用两种方式：一种方式是在线自动更新。对于证书信息无须改变的订户，在证书即将过期时，在获得 FJCA 授权后，自助进行在线证书更新操作，获得新证书。

另一种方式是人工方式更新。对于证书信息发生改变的订户，由注册机构来处理证书更新请求，为订户制作新的证书。

注册机构对申请证书更新订户的进行查验与鉴别，鉴别要求同本《电子认证业务规则》3.2.2 和 3.2.3。

4.7.4 颁发新证书对订户的通告

在线自动更新方式，在自动完成更新，给订户颁发新证书时，在线更新系统会自动通知证书更新已完成，新证书已颁发。

人工更新方式，对订户的通告有以下几种方式：

- a) 通过面对面的方式，通知证书更新已完成，新证书已颁发；
- b) 邮政信函通知订户；
- c) 其他 FJCA 认为安全可行的方式通知订户。

4.7.5 构成接受密钥更新证书的行为

在线更新方式，当订户对在线系统提示证书更新已完成，新证书已颁发进行确认时，就表示订户接受更新证书。

人工更新方式，当更新证书签发后，注册机构将证书及其密码信封当面或寄送给订户，就表示订户接受更新证书。

4.7.6 电子认证服务机构对密钥更新证书的发布

FJCA 在签发密钥更新证书后，就将更新证书发布到数据库和目录服务器中，对外进行发布。

4.7.7 电子认证服务机构对其他实体的通告

其他实体可以通过从目录服务器中查询已更新的数字证书。

4.8 证书变更

4.8.1 证书变更的情形

- a) 证书的主体内容发生改变；
- b) 证书的 E-mail 地址发生改变；
- c) 其他。

4.8.2 请求证书变更的实体

订户可以请求证书变更。订户包括持有 FJCA 签发的个人、组织及设备等各类证书的证书持有人。

4.8.3 证书变更请求的处理

处理证书变更请求可以采用两种方式：一种方式是在线自动变更。对于证

书信息无须改变的订户，在证书 E-mail 地址发生改变时，在获得 FJCA 授权后，自助进行在线证书更新操作，获得新证书。

另一种方式是人工方式更新。对于证书信息发生改变的订户，由注册机构来处理证书更新请求，为订户制作新的证书。

注册机构对申请证书更新订户的进行查验与鉴别，鉴别要求同本《电子认证业务规则》3.2.2 和 3.2.3。

4.8.4 颁发新证书时对订户的通告

在线自动更新方式，在自动完成更新，给订户颁发新证书时，在线更新系统会自动通知证书更新已完成，新证书已颁发。

人工更新方式，对订户的通告有以下几种方式：

- a) 通过面对面的方式，通知证书更新已完成，新证书已颁发；
- b) 邮政信函通知订户；
- c) 其他 FJCA 认为安全可行的方式通知订户。

4.8.5 构成接受变更证书的行为

在线更新方式，当订户对在线系统提示证书更新已完成，新证书已颁发进行确认时，就表示订户接受变更新证书。

人工更新方式，当更新证书签发后，注册机构将证书及其密码信封当面或寄送给订户，就表示订户接受更新证书。

4.8.6 电子认证服务机构对变更证书的发布

FJCA 在签发变更新证书后，就将变更新证书发布到数据库和目录服务器中，对外进行发布。

4.8.7 电子认证服务机构对其他实体的通告

其他实体可以通过从目录服务器中查询已更新的数字证书。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

- a) 发生下列情形之一的，订户应当申请吊销数字证书：
 - 1) 数字证书私钥泄露；
 - 2) 数字证书中的信息发生重大变更；
 - 3) 认为本人不能实际履行数字证书认证业务规则。
- b) 发生下列情形之一的，FJCA 可以吊销其签发的数字证书：
 - 1) 订户申请吊销数字证书；
 - 2) 订户提供的信息不真实；
 - 3) 订户没有履行双方合同规定的义务；
 - 4) 数字证书的安全性得不到保证；
 - 5) 法律、行政法规规定的其他情形。

4.9.2 请求证书吊销的实体

根据不同的情况，订户、FJCA、注册机构可以请求吊销最终用户证书。

4.9.3 吊销请求的流程

证书吊销请求的处理采用与原始证书签发相同的过程。

- a) 证书吊销的申请人到 FJCA 授权的注册机构书面填写《证书吊销申请表》，并注明吊销原因；
- b) FJCA 授权的注册机构根据 3.2 的要求对订户提交的吊销请求进行审核；
- c) FJCA 吊销订户证书后，注册机构将当面通知订户证书被吊销，订户证书在 24 小时内进入 CRL，向外界公布；
- d) 强制吊销是指当 FJCA 或 FJCA 授权的注册机构确认用户违反本《电子认证业务规则》的情况发生时，对订户证书进行强制吊销，吊销后将立即通知该订户。

4.9.4 吊销请求宽限期

如果出现私钥泄露等事件，吊销请求必须在发现泄露或有泄露嫌疑 8 小时内提出。其他吊销原因的吊销请求必须在 48 小时内提出。

4.9.5 电子认证服务机构处理吊销请求的时限

发证机构接到吊销请求后立即处理，24 小时生效。FJCA 每日签发一次 CRL，并将最新的 CRL 发布到目录服务器指定的位置，供请求者查询下载。

CRL 的结构如下：

- 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/吊销日期(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)

4.9.6 依赖方检查证书吊销的要求

在具体应用中，依赖方必须使用以下两种功能之一进行所依赖证书的状态查询：

a) 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。

b) 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。注意：依赖方要验证 CRL 的可靠性和完整性，确保是经 FJCA 发布并且签名的。

4.9.7 CRL 的颁发频率

FJCA 可采用定期的方式发布 CRL。颁发 CRL 的频率根据证书策略确定，每小时自动发布最新 CRL，如遇特殊情况，人工发布最新 CRL。

4.9.8 CRL 发布的最大滞后时间

一个证书从它被吊销或它被发布到CRL上的滞后时间不超过24小时。

4.10 证书状态服务

4.10.1 操作特点

FJCA 通过目录服务器为用户提供证书状态服务。

4.10.2 服务可用性

FJCA 提供 7X24 小时的证书状态查询服务。即在网络允许的情况下，订户能够实时获得证书状态查询服务。

4.10.3 可选特征

根据请求者的要求，在请求者支付相关费用后，FJCA 可以提供以下通知服务：

- a) 收到证书主题的电子签名消息的接受者要求，确认该证书是否已被吊销；
- b) 提供通知服务，当指定的证书被吊销时，FJCA 将通知请求该项服务的请求者。

4.11 订购结束

订购结束是指当证书有效期满或证书吊销后，该证书的服务时间结束。

订购结束包含以下两种情况：

a) 证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，订户可以终止订购；

b) 在证书有效期内，证书被吊销后，即订购结束。

4.12 密钥生成、备份与恢复

4.12.1 密钥生成、备份与恢复的策略和行为

订户的签名密钥对由订户的密码设备（如智能 USB KEY 或智能 IC 卡）生成，加密密钥对由密钥管理中心生成。

签名密钥对由订户的密码设备保管。

密钥恢复是指加密密钥的恢复，密钥管理中心不负责签名密钥的恢复。密钥恢复分为两类：订户密钥恢复和司法取证密钥恢复。

a) 订户密钥恢复：当订户的密钥损坏或丢失后，某些密文数据将无法还原，此时订户可申请密钥恢复。订户在 FJCA 授权的发证机构申请，经审核后，通过 FJCA 向 KMC 请求；密钥恢复模块接受订户的恢复请求，恢复订户的密钥并下载于订户证书载体中。

b) 司法取证密钥恢复：司法取证人员在 KMC 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。

具体策略在 6.1 和 6.2 中详细描述。

4.12.2 会话密钥的封装与恢复的策略和行为

非对称算法组织数字信封的方式来封装会话密钥。数字信封使用信息接受者的公钥对会话密钥加密，接受者用自己的私钥解开并恢复会话密钥。

5. 电子电子认证服务机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

a) FJCA 的建筑物和机房建设按照下列标准实施：

- 1) GB 50174-93: 《电子计算机机房设计规范》
- 2) GB 2887-89: 《计算站场地技术条件》
- 3) GB 9361-88: 《计算站场地安全要求》
- 4) GB 6650-1986: 《计算机机房用活动地板技术条件》
- 5) GB 50034-1992: 《工业企业照明设计标准》
- 6) GB 5054-95: 《低压配电装置及线路设计规范》
- 7) GBJ 19-87: 《采暖通风与空气调节设计规范》
- 8) GB 157: 《建筑防雷设计规范》
- 9) GBJ 79-85: 《工业企业通信接地设计规范》

b) FJCA 机房位于福建省福州市温泉公园路 188 号，实行分层访问的安全管理：FJCA 的功能区域划分为七个层次，四个区域。

七个层次由外到里分别是：入口、办公、敏感、缓冲、数据中心、屏蔽机房、保密机柜。

四个区域由外到里分别是：公共区域、DMZ 区域（非军事区）、操作区域和安全区域。

其中，入口之外的区域为公共区域，入口和办公层位于 DMZ 区，敏感层位于操作区，其他各层位于安全区。

5.1.2 物理访问

为了保证本系统的安全，采取了一定的隔离、控制、监控手段。机房的所有门都足够结实，能防止非法的进入。机房通过设置门禁和侵入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：

a) 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纪录和信息提示。

b) 报警系统：当发生任何非法闯入、非正常手段的开门、长时间不关门等异常情况都应触发报警系统。报警系统明确指出报警位置。

c) 监控系统：与门禁和物理侵入报警系统配合使用的还有录像监控系统，对安全区域和操作区域进行 24 小时不间断录像。所有录像资料需要保留，以备查询。

门禁和物理侵入报警系统备有 UPS，并提供至少 8 小时的不间断供电。

5.1.3 电力与空调

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统，按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备分开供电。供配电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。计算机设备专用配电柜和辅助设备配电柜独立设置。

使用不间断电源（UPS）来保证供电的稳定性和可靠性。采用双电源，在单路电源损坏时，可以自动切换，维持系统正常运转。

根据机房环境及设计规范要求，主机房和基本工作间，均设置了空气调节系统。空调系统使用独立空调。其组成包括空调、通风管路、新风系统。

FJCA 的要求参照电信设施管理的规定，而且每年对物理系统的安全性进行检查。

5.1.4 水患防治

机房内无渗水、漏水现象，主要设备采用专用的防水插座，并采取必要措施防止下雨或水管破损，造成天花板漏水、地板渗水和空调漏水等现象。

FJCA 的系统有充分保障，能够防止水侵蚀。

目前机房内无上下水系统，空调间做了严格防水处理，由漏水检测系统提

供（7X24）实时检测。

5.1.5 火灾防护

火灾预防：

a) 敏感区（物理三层）、高度敏感区域（物理四、五、六层），其建筑物的耐火等级符合 GBJ45《高层民用建筑设计防火规范》中规定的二级耐火等级。

b) FJCA 设施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。

c) 敏感区及高敏区配置独立的气体灭火装置，使用七氟丙烷（HFC-227ea）等洁净气体灭火系统，备有相应的气体灭火器，非敏感区根据实际情况可配置水喷淋灭火装置。FJCA 内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。

d) 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。

e) 火灾自动灭火设施的区域内，其隔墙和门的耐火极限不低于 1 小时，吊顶的耐火极限不得低于 15 分钟。

f) 在非敏感区及敏感区的办公区域内，须设置紧急出口，紧急出口必须设有消防门，消防门符合安全要求。紧急出口门外部不能有门开启的装置，且紧急出口门须与门禁报警设备联动外，需装配独立的报警设备。

g) 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。FJCA 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。

灭火系统采用电动，手动，紧急启动三种方式：

a) 电动方式：防护区报警系统第一次火警确认后，发出声光警示信号，切断非消防电源（如：空调电源、照明电源等）。并送排风（烟），防火阀关闭。第二次火警确认后，经延时，同时发出气体释放信号，并发出启动电信号，送给对应的管网启动钢瓶，喷气灭火。

b) 手动方式：人员对钢瓶或药剂瓶直接开启操作。

c) 紧急启动：防护区外设有紧急启动按钮供紧急时使用。

FJCA 通过与专业防火部门协调，实施消防灭火等应急响应措施。

5.1.6 介质存储

FJCA 的存储介质包括硬盘、软盘、磁带、光盘等，介质存储地点和 FJCA 系统分开并且保证物理安全，注意防磁、防静电干扰、防火、防水，由专人管理。

5.1.7 废物处理

当 FJCA 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。写在纸张之上的，必须切碎或烧毁。如果保存在磁盘中，应多次重写覆盖磁盘的存储区域，其他介质以不可恢复原则进行相应的销毁处理。

5.1.8 异地备份

FJCA 对认证系统的核心数据，采用同城异地的的方式进行备份，为此，专门制定了异地备份管理制度。按规定每周执行一次，备份数据由专人护送指定地方。异地数据备份安全要求都符合 FJCA 备份标准和程序。

5.2 程序控制

5.2.1 可信角色

FJCA 明确执行 CA 关键职能员工及独立合约人，均视为可信角色，具体包括：

1、超级管理员

超级管理员由 FJCA 运营安全管理小组任命，共有 5 名分别掌管着 CA 系统初始化时生成的 5 个主用户卡，是认证系统安全运行和管理的核心。

超级管理员负责导入 CA 根证书，以及对系统管理员、安全管理员、审计管理员、密钥管理员、网络管理员、各级制证员和独立合约人的角色增加、角色注销、角色权限设置、角色权限修改工作。

超级管理员具有系统访问权限、其他可信角色的设置权限，以及可信角色相应权限的分配权。至少 3 名超级管理员同时在场并许可的情况下，通过 3 张主用户卡设置其他可信角色以及为其他可信角色授权。

2、系统管理员

FJCA 运营安全管理小组负责任命系统管理员角色，并签发《任命单》、《责任表单》和《访问授权表单》，其设置和权限分配是由 5 名超级管理员（按照 5 选 3 多人控制，至少 3 名在场并许可）通过主用户卡生成的。

系统管理员负责系统的日常维护、参数调整、备份、异常事件处理以及与进程有关的系统监控工作，同时根据超级管理员的授权签发各级制证员证书。

系统管理员具有对各级制证员证书的执行权限，以及系统维护和系统数据的查询、统计、分析权限。

3、安全管理员

安全管理员是由 FJCA 运营安全管理小组任命，由 5 名超级管理员（按照 5 选 3 多人控制，至少 3 名在场并许可）通过主用户卡生成的。

安全管理员对 FJCA 的安全管理进行定期检查和评估，并根据评估结果对安全策略和执行程序进行修订和维护。

安全管理员有权定义并指定 FJCA 中某特定个人和部门的安全职责。

4、审计管理员

审计管理员是由 FJCA 运营安全管理小组任命，由 5 名超级管理员（按照 5 选 3 多人控制，至少 3 名在场并许可）通过主用户卡生成的。

审计管理员负责定期对 FJCA 的可信角色、物理安全、通信安全、操作安全及系统安全进行审计检查，安全审计系统分布于证书管理系统的各个子系统中，以保障整个系统的安全运行。

审计管理员拥有对系统事件/日志进行查询、备份、追踪、报告、汇总、删除的权限。

5、密钥管理员

密钥管理员是由 FJCA 运营安全管理小组任命，由 5 名超级管理员（按照 5 选 3 多人控制，至少 3 名在场并许可）通过主用户卡生成的。

密钥管理员负责管理 FJCA 密钥相关设备，进行 FJCA 密钥的申请、使用监

控、配合国家密码主管部门的工作人员进行密钥的生成、备份、恢复等操作。

密钥管理员具有证书操作的执行权限。

6、网络管理员

网络管理员是由 FJCA 运营安全管理小组任命，由系统管理员根据任命授权并执行的。

网络管理员负责对 FJCA 的网络相关设备及线路的维护和管理，进行线路调整、设备配置更改、设备更换、网络安全防护等操作，保证数字证书服务体系的正常运转。

网络管理员仅具备系统网络及设备的维护和管理权限。

7、制证员

制证员是由 FJCA 运营安全管理小组任命，由系统管理员根据任命授权并执行的。

按制证员的不同级别分别负责订户数字证书的录入、审核、制作、更新、吊销等证书业务操作，直接对订户提供服务。

5.2.2 每项任务需要的人数

FJCA 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。

FJCA 确保单个人不能接触、导出、恢复、更新、撤销 CA 存储的 CA 证书对应的私钥。至少三个人，使用一项对参加操作人员保密的密钥分割和合成技术，来进行任何密钥恢复的操作。

进入 KMC 和 CA 安全区需要两名以上（含两名）有访问权限的人员；

操作存放有根密钥的密码设备，至少需要五个密码分割持有人。

5.2.3 每个角色的识别与鉴别

所有 FJCA 的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡和指纹识别；进入系统需要使用数字证书进行身份鉴别。FJCA 将独立完整地记录其所有的操作行为。

5.2.4 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。FJCA对如下人员进行了职责分割：

- I 超级管理员
- I 系统管理员
- I 安全管理员
- I 审计管理员
- I 网络管理员
- I 密钥管理员
- I 制证员

订户证书的录入、审核、签发操作的签证官不能由同一个人进行。

5.3 人员控制

5.3.1 资格、经历和无过失要求

所有的员工与 FJCA 签订保密协议。对于充当可信角色或其他重要角色的人员，必须具备的一定的资格，具体要求在人事管理制度中规定。FJCA 要求充当可信角色的人员至少必须具备忠诚、可信赖及工作的热诚度、无影响 CA 运行的其它兼职工作、无同行业重大错误记录、无违法记录等。

5.3.2 背景审查程序

FJCA 与有关的政府部门和调查机构合作，完成对 FJCA 可信任员工的背景调查。

所有目前的可信任员工和申请调入的可信任员工都必须书面同意对其进行背景调查。

背景调查分为：基本调查和全面调查。

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) 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。
- d) 经考核，人事部门和用人部门联合填写《可信雇员调查表》，报主管领导批准后准予上岗。

5.3.3 培训要求

FJCA 对运营人员按照其岗位和角色安排不同的培训。培训有：系统硬件安装与维护、系统软件运行与维护、系统安全、应用软件的运行和维护、CA 中心的运行管理、CA 中心的内部管理、政策和规定及系统备份与恢复等。

对于运营人员，其 CA 的相关知识技能，每年至少要总结一次并由 FJCA 组织培训。技术的进步、系统功能更新或新系统的加入，都需要对相关人员进行培训。

5.3.4 再培训周期和要求

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

认证策略调整、系统更新时，应对全体人员进行再培训，以适应新的变化。

5.3.5 工作岗位轮换周期和顺序

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

5.3.6 对未授权行为的处罚

当 FJCA 员工被怀疑，或者已进行了未授权的操作，例如滥用权利或超出权限使用 FJCA 系统或进行越权操作，FJCA 得知后将立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。对情节严重的，依法追究相应责任。

5.3.7 独立合约人的要求

对不属于 FJCA 内部的工作人员，但从事 FJCA 有关业务的人员等独立签约者(如注册机构的工作人员)，FJCA 的统一要求如下：

- a) 人员档案进行备案管理；
- b) 具有相关业务的工作经验；
- c) 必须接受 FJCA 组织的为期一周的岗前培训。

5.3.8 提供给员工的文档

为使得系统正常运行，必须提供给具有权限的相关人员各种文档，包括：

- a) 加密机用户手册；
- b) 机房设备管理办法；
- c) 密码信封打印工具用户手册；
- d) 数字证书运营规范；
- e) 灾难备份和恢复方案；
- f) 目录服务器安装配置手册。

5.4 审计日志程序

5.4.1 记录事件的类型

FJCA 记录与系统相关的事件，这些记录信息称为日志。对于这些日志，无论其载体是纸张还是电子文档的形式，必须包含事件发生的日期、事件的发生时

间段、事件的内容和事件相关的实体等。

FJCA 还可能记录与系统不直接相关的事件，例如：物理通道参观记录、人事变动等。

5.4.2 处理日志的周期

FJCA 每周对日志进行审查，并对审查日志的行为进行备案。

5.4.3 审计日志的保存期限

审计日志的数据库记录保存三个月，纸质文件保存五年。异常情况记录和报表的保存至少十年。

5.4.4 审计日志的保护

FJCA 执行严格的管理，确保只有 FJCA 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、修改和删除等操作，另外对日志要进行异地备份。审计日志的制作和访问进行岗位分离。

FJCA 将审计日志存储到磁带中，并存放到异地，实行安全保管。

5.4.5 审计日志备份程序

FJCA 保证所有的审查记录和审查总结都按照 FJCA 备份标准和程序进行备份。根据记录的性质和要求，分为实时、按天、按周、按月和按年等多种形式的备份，可采用在线和离线两种方式的备份工具。

审计文档由管理员每周进行一次归档。所有档案安全存放在文档库内。

5.4.6 审计日志收集系统

审计日志收集系统涉及：

I 证书管理系统；

- I 证书签发系统;
- I 证书目录系统;
- I 远程通信系统;
- I 证书受理系统;
- I 访问控制系统;
- I 网站、数据库安全管理系统;
- I 其他需要审计的系统。

FJCA 使用审计工具满足对上述系统审计的各项要求。

5.4.7 对导致事件实体的通告

导致事件主要包括攻击和非授权行为。

FJCA对审查中发现的攻击现象将做详细记录,在法律许可的范围内追溯攻击者,并保留采取相应对策措施的权利,如:切断对攻击者已经开放的服务、递交司法部门处理等措施。

FJCA对审查中发现的未授权行为将上报FJCA运营安全管理小组,取消该员工相关授权,并对未授权行为进行评估,确认风险,做出相应处理。

5.4.8 脆弱性评估

FJCA至少每年要进行系统、物理场地、运营管理、人事管理等方面的安全脆弱性评估,并根据评估报告采取措施,以降低系统运行的风险。

5.5 记录归档

5.5.1 归档记录的类型

归档记录包括所有审计数据、证书申请信息、与证书申请相关的信息等。

5.5.2 归档记录的保存期限

除了法律法规和电子认证服务主管机构规定的保存期限以外,FJCA 制定的

有关归档保存期如下：

- 1、订户服务申请的信息，如申请表和其他相关信息的记录，保存期限至少为电子签名认证证书失效后五年；
- 2、认证系统日常运作产生的日志记录等文件保存 3 年；
- 3、机房进出记录、认证系统日常维护记录、系统软硬件设备更换、安装、拆除、配置变化等的记录、系统的故障处理记录等保存 3 年；
- 4、机房监控系统记录保存 1 年；
- 5、订户申请、更新、吊销、挂起的证书和过期证书，永久保存；FJCA 的证书和密钥，以及相关的变动信息，永久保存；
- 5、人员变更记录等保存 5 年；
- 6、与法律政策的规定不一致的，选择两者中较长的期限予以保存。

5.5.3 归档文件的保护

存档内容既有物理安全措施的保证，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查询。FJCA 保护相关的档案内容，免遭恶劣环境的威胁，如温度、湿度和强磁力等的破坏。

5.5.4 归档文件的备份程序

所有存档的文件和数据库除了保存在 FJCA 的存储库，还在异地保存其备份。存档的数据库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。FJCA 在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

5.5.5 记录时间戳要求

FJCA 的归档文件和记录，都有日期标识，有些是系统自动产生记录，有些是业务人员手动增加。

5.5.6 获得和检验归档信息的程序

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

5.6 电子认证服务机构密钥更替

电子认证服务机构密钥更替指 FJCA 根证书到期和电子认证服务机构证书到期时，需要更换密钥而采取的措施。

a) FJCA 根密钥由加密机产生，有效期为 15 年，更替办法为：

使用旧的私钥对新的公钥及信息签名生成证书；

使用新的私钥对旧的公钥及信息签名生成证书；

使用新的私钥对新的公钥及信息签名生成证书。

通过以上 3 张证书达到密钥更换的目的，使新旧证书之间互相信任。

b) 电子认证服务机构证书到期之前，FJCA 将采取以下方式更替：

FJCA 将在证书到期前的 60 天内停止颁发新的证书；

旧的证书到期后，FJCA 将用新的密钥对签发证书。

密钥更替时直接把当前 CA 证书吊销，签发到 ARL 并发布，然后签发一个新的 CA 证书，通过证书库和 LDAP 方式下发给证书应用系统。

c) FJCA 将继续使用旧的根私有密钥签发的 CRL，直到旧的私钥签发的证书到期为止。

5.7 损害和灾难恢复

为了在出现异常或者灾难情况时，能够在最短的时间内重恢复认证系统的运行，FJCA 制定了可靠的损害和灾难恢复计划，以应对突发事故导致的系统问题。

5.7.1 事故和损害处理程序

FJCA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，FJCA将按照灾难恢复计划实施修复。具体由FJCA灾难恢复计划决定。

FJCA承诺：保证在发生灾难24小时之内恢复目录查询服务，一个月之内恢复证书签发和证书管理服务。在数据恢复中，最多允许丢失发生灾难后48小时内数据。

5.7.2 计算资源、软件和/或数据的损坏

当认证系统运营使用的软件、数据或者其他信息出现异常损毁时，可以依照FJCA的灾难恢复计划，根据系统内部备份的资料，或者异地备份的资料，执行系统恢复操作，使认证系统能够重新正常运行。

当认证系统使用的硬件设备出现损毁时，可以依照灾难恢复计划，启动备份硬件设备以及相关的备份操作系统和认证系统，重新恢复系统运行。

FJCA应在6小时内完成恢复过程，如果无法在6小时内完成恢复过程，则应启动备份机制，在24小时内恢复系统运行。

5.7.3 实体私钥损害处理程序

FJCA的根私钥出现损毁、遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，FJCA应该：

- 1、立即向工业和信息化部和相关政府主管部门汇报，并立即吊销所有已经被签发的证书，更新CRL和OCSP信息，供订户和依赖方查询。同时FJCA立即生成新的密钥对，并自签发新的根证书。

- 2、新的根证书签发以后，按照本CPS关于证书签发的规定，重新签发下级证书和FJCA下级子CA证书。

- 3、FJCA新的根证书签发以后，将会立即通过FJCA信息库、网站等方式进行发布。

订户的私钥出现遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，订户应该按照本CPS的规定，首先申请证书吊销，并按照规定重新申请新的证书。

5.7.4 灾难后的业务连续性能力

为避免突发灾难造成认证业务停顿，FJCA应制订一套完整的异地业务恢复计划，并建立相应的异地灾难备份系统，将认证系统运行所需要的软硬件设备、数据存储、证书和用户信息、业务操作规范和灾难恢复文件，在离开现有运行系统适当距离的异地备份中心，建立备份系统。

异地备份中心的认证业务恢复系统，根据需要每年将至少开展一次灾难恢复计划的演练，并根据实际情况的变化，及时更新恢复计划和灾难恢复文件，并保存相应的归档纪录。从而保证在出现灾难时，认证系统能够在24小时内恢复系统运行和服务提供。

5.8 电子认证服务机构或注册机构的终止

因各种情况，FJCA 需要终止运营时，将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

FJCA 在终止服务九十日前，就业务承接及其他有关事项通知有关各方，包括但不限于 FJCA 授权的发证机构和订户等。

在终止服务六十日前向中华人民共和国工业和信息化部报告，按照相关法律规定的步骤进行操作。

FJCA 采用以下措施终止业务：

- a) 起草 FJCA 终止业务声明；
- b) 停止认证中心所有业务；
- c) 处理加密密钥；
- d) 处理和存档敏感文件；
- e) 清除主机硬件；
- f) 管理 FJCA 系统管理员和安全官员；
- g) 通知与 FJCA 终止运营相关的实体。

根据 FJCA 与注册机构签订的运营协议终止注册机构的业务。

6. 认证系统技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

订户的签名密钥对由订户的密码设备（如智能 USB KEY 或智能 IC 卡）生成，加密密钥对由 KMC 生成。

6.1.2 私钥传送给订户

订户的签名密钥对由自己的密码设备生成并保管。

加密密钥对由 KMC 产生，通过安全通道传到订户手中的密码设备中。

6.1.3 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道，经注册机构传递到 FJCA。

订户的加密证书公钥，由 KMC 通过安全通道传递到 CA 中心。

从 RA 到 CA 以及从 KMC 到 CA 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 电子认证服务机构公钥传送给依赖方

依赖方可以从 FJCA 的网站(<http://www.fjca.com.cn>)下载根证书和 CA 证书，从而得到 CA 的公钥。

6.1.5 密钥的长度

FJCA 用于加密和签名的非对称密钥对的模长是 1024 比特，对称密钥的长度是 128 比特。

6.1.6 公钥参数的生成和质量检查

公钥参数由国家密码管理局许可的硬件产生。

6.1.7 密钥使用目的

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。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块标准和控制

FJCA 所用的密码设备都是经国家相关部门认可的产品，其安全性达到以下要求：

接口安全：不执行规定命令以外的任何命令和操作；

协议安全：所有命令的任意组合，不能得到私钥的明文；

密钥安全：密钥的生成和使用必须在硬件密码设备中完成；

物理安全：密码设备具有物理防护措施，任何情况下的拆卸均立即销毁在设备内保存的密钥。

6.2.2 私钥的多人控制

根 CA 系统的私钥的生成、更新、吊销、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 5 张管理员卡中，只有其中三至五人在场并许可的情况下，才能对私钥进行上述操作。

订户的私钥由订户自己通过密码设备控制。

6.2.3 私钥托管

订户加密证书对应的私钥由密钥管理中心托管，订户的签名证书对应的私钥由自己保管，密钥管理中心不负责托管。

KMC 严格保证用户密钥对的安全，密钥以密文形式保存，密钥库具有最高安全级别，禁止外界非法访问。

6.2.4 私钥备份

订户的签名密钥 FJCA 和 KMC 都不备份。加密私钥由 KMC 备份，备份数据以密文形式存在。

6.2.5 私钥归档

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

FJCA 提供过期的托管加密密钥的归档服务。

6.2.6 私钥导入、导出密码模块

使用 FJCA 软件可以把私钥安全导入到密码模块中，私钥无法从硬件密码模块中导出。

6.2.7 私钥在密码模块中的存储

私钥在硬件密码模块中加密保存。

6.2.8 激活私钥的方法

具有激活私钥权限的管理员使用含有自己的身份的加密 IC 卡登录，启动密钥管理程序，进行激活私钥的操作，需要三名管理员同时在场。

6.2.9 解除私钥激活状态的方法

具有解除私钥激活状态权限的管理员使用含有自己的身份的加密 IC 卡登录，启动密钥管理程序，进行解除私钥的操作，需要三名管理员同时在场。

6.2.10 销毁密钥的方法

具有销毁密钥权限的管理员使用含有自己的身份的加密 IC 卡登录，启动密钥管理程序，进行销毁密钥的操作，需要三名管理员同时在场。

6.2.11 密码模块的评估

FJCA 使用山大得安的 SJY05-B 服务器密码机，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。主要技术指标如下：

- a) 通信接口：符合国际 ITU Ethernet RJ45 标准；
- b) 带宽控制：10M/100M 自适应，充分满足突发业务需要；
- c) 并发容量：可支持同时并发 100 个的独立安全处理容量；
- d) 密钥管理：密钥不以明文形式出现在服务器密码机以外；通信密钥通过 RSA 身份鉴别后协商得到；
- e) 身份鉴别：采用用户 IC 卡对用户进行身份鉴别管理，以控制对加密系统的使用；
- f) 处理速度：数据加解密处理能力为 15.6Mbps；
模长 1024 的数字签名速度 105 次/秒。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

订户证书中的公钥包括签名证书中的公钥和加密证书中的公钥。它们由 FJCA 和密钥管理中心定期归档。

6.3.2 证书操作期和密钥对使用期限

所有订户证书的有效期和其对应的密钥对的有效期都是一致的。

6.4 激活数据

6.4.1 激活数据的产生和安装

激活数据是私钥保护密码，证书存储介质（如：智能 KEY）出厂时设置了缺省的 PIN 值，证书制作时将此 PIN 值更改为密码信封中的密码，从而激活了证书存储介质的 PIN。

6.4.2 激活数据的保护

证书存储介质的 PIN 值用密码信封中的密码进行保护。

6.4.3 激活数据的其他方面

只有在拥有证书介质并知道证书介质的 PIN 值时才能激活证书存储介质，进而使用私钥。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

为了保证系统的正常运行，对所需要的计算机设备进行正确的选型、验收，制定操作规范。另外，本系统采用增加冗余资源的方法，使系统在有故障时仍能正常工作。

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，必须有派专人在场监督。

6.5.2 计算机安全评估

FJCA 证书系统已通过国家密码管理委员会办公室组织的商用密码产品技术鉴定，证书编号：国密证第 0102 号。

6.6 生命周期技术控制

6.6.1 系统开发控制

系统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，系统的容错设计采用多路并发容错方式，确保系统在出错的时候尽可能不停止服务。

6.6.2 安全管理控制

FJCA 对系统的维护保证操作系统、网络设置和系统配置安全。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。

6.6.3 生命周期的安全控制

整个系统从设计到实现，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，使用的算法和密码设备均通过了主管部门鉴定，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、密钥恢复等安全运行措施，整个系统安全可靠。

6.7 网络的安全控制

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

6.8 时间戳

时间戳系统提供的时间戳服务在技术实现上严格遵循国际标准时间戳协议 (RFC3161)，采用标准的时间戳请求、时间戳应答以及时间戳编码格式，时间源采用国家授时中心提供的标准时间。

7. 证书、证书吊销列表和在线证书状态协议

7.1 证书

FJCA 签发的证书符合 X.509 V3 格式。遵循 RFC3280 标准。

7.1.1 版本号

X.509 V3。

7.1.2 证书扩展项

FJCA 证书扩展项除使用 IETF RFC 3280 中定义的证书扩展项，还支持私有扩展项。

FJCA 采用的 IETF RFC 3280 中定义的证书扩展项：

- I 颁发机构密钥标识符 Authority Key Identifier
- I 主体密钥标识符 Subject Key Identifier
- I 密钥用法 Key Usage
- I 扩展密钥用途 Extended Key Usage

- I 私有密钥使用期 Private Key Usage Period
 - I 主体可选替换名称 Subject Alternative Name
 - I 基本限制 Basic Constraints
 - I 证书撤销列表分发点 CRL Distribution Points
- 私有扩展项可支持以下类型：
- I 个人身份证号码 Identify Card Number
 - I 企业工商注册号 IC Registration Number
 - I 企业组织机构代码 Organization Code
 - I 企业税号 Taxation Number

7.1.3 算法对象标识符

使用 SHA1WithRSAEncryption 算法

算法 OID 1.2.840.113549.1.1.5

7.1.4 名称形式

FJCA 数字证书中的主体 Subject 的 X.500 DN 是 C=CN 命名空间下的 X.500 目录唯一名字，各属性的编码一律使用 UTF8String。

主体 Subject 的 X.500 DN 支持多级 O 和 OU，其格式如下：

C=CN;

O=××

O=××

OU=××;

OU=××;

CN=××

I C (Country) 应为 CN，表示中国；

I O (Organization) 中的内容分为 2 种：

- a) 证书主体或者证书主体所属单位具有明确的上一级单位，则应为其上一级单位的名称全称；

b) 不存在 a) 中所述的上一级单位，则应为证书主体或者证书主体所属单位的所在省、自治区、直辖市名称全称；

I OU (Organization Unit) 应为证书主体或者证书主体所属单位的名称全称；

I CN (Common Name) 中的内容分为 4 种：

a) 个人证书中应为证书主体的姓名；

b) 单位机构证书中应为证书主体单位的标准简称；

c) 服务器证书应为证书主体设备的域名或者 IP 地址或者设备编码；

d) 代码签名证书应为负责人的姓名，或者是所属单位的标准简称；

Email 仅在邮件证书的 DN 中存在，应为证书主体的有效电子邮件地址。

7.2 证书吊销列表

FJCA 签发的证书吊销列表符合 X.509 V2 格式。遵循 RFC3280 标准。

7.2.1 版本号

X.509 V2。

7.2.2 CRL 和 CRL 条目扩展项

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

CRL 条目扩展项：不使用 CRL 条目扩展项

7.3 在线证书状态协议

7.3.1 版本号

使用 OCSP 版本 1 (OCSP v1)。

7.3.2 OCSP 扩展项

不使用 OCSP 扩展项。

8. 电子认证服务机构审计和其他评估

8.1 评估的频率或情形

FJCA 在如下情形中进行评估：

1、根据中华人民共和国电子签名法和电子认证服务管理办法等的要求，每年，接受主管部门的评估和检查。

2、FJCA 根据国家主管部门要求及相关标准制定本 CPS 的规定运营和服务，进行内部评估和审计，每年至少执行一次内部的评估审核。

3、其他评估。

(1) 年度评估：由 FJCA 邀请第三方的审计机构每年进行评估；

(2) 运营前评估：在新系统向公众提供服务前由行业主管部门对新系统进行评估，评估合格后方可正式运营。

8.2 评估者的资质

FJCA 自己组织的内部审计人员须具备如下条件：

- 1) 具备信息安全审计的相关知识，有两年以上的相关经验；
- 2) 熟悉本CPS的规范；
- 3) 具备计算机、网络、信息安全等方面的知识和实际工作经验。

自行的内部审计由FJCA运营安全管理小组负责组织实施，并确定审计人员。

协助FJCA进行内部审计的第三方审计机构所具有的资质和经验必须符合法律和行业准则规定的要求，包括：

I 必须是经许可成立的、有营业执照的、具有计算机安全专门技术知识的的审计人员或审计评估机构，且在业界享有良好的声誉。

I 了解计算机信息安全体系、通信网络安全要求、PKI技术、标准和操作。

- I 具备检查系统运行性能的专业技术。

8.3 评估者与被评估者之间的关系

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。

8.4 评估内容

1、FJCA按照工业和信息化部依法提出的评估要求和规范，接受其任何内容的评估。

2、FJCA内部评估审核的内容包括：

- I 是否制订和公布CPS；
- I 是否按照CPS来制订相关的操作规范和操作流程；
- I 是否接受对所有流程和操作的审计；
- I 是否按照本CPS及相关操作规范和操作流程开展业务；
- I 是否符合本CPS及与之相关的授权协议；
- I 服务的完整性；
- I 物理与环境安全控制；
- I 系统与网络安全控制；
- I 人员的安全控制；
- I 建筑设施的安全控制；
- I 软硬件设备的存储介质的安全控制；
- I 系统开发和维护的安全控制；
- I 灾难恢复和备份系统的管理；
- I 审计和归档的安全管理；

8.5 对问题与不足采取的措施

如果审计报告显示任何实质性的不符合要求时，CA、RA 必须制定改善计划。如果 CA、RA 没有针对审计报告采取适当的改进措施，FJCA 必须暂时停止 CA、RA

对公众提供服务。FJCA 将根据国际惯例和相关法律、法规迅速解决问题。

8.6 评估结果的传达与发布

1、工业和信息化部在完成审查后，按照法律法规的要求对审查结果进行改进完善。

2、FJCA 有权利决定是否将审查结果公布。

9. 法律责任和其他业务条款

9.1 费用

9.1.1 证书签发和更新费用

数字证书的收费标准按照国家和福建省物价主管部门批准的收费标准执行。根据证书实际应用的需要，FJCA 在不高于收费标准的前提下可以对证书价格进行适当调整。

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，FJCA 不收取查询费用。

9.1.3 证书吊销或状态信息的查询费用

查询证书是否吊销，FJCA 不收取信息访问费用。

对于在线证书状态查询(OCSP)，由 FJCA 与订制者在协议中约定。

9.1.4 其他服务的费用

FJCA 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

在实施证书操作和签发证书的过程中，FJCA 遵守并保持严格的操作程序和策略。一旦订户接受数字证书，FJCA 将不办理退证、退款手续。

如果订户在证书服务期内退出数字证书服务体系，FJCA 将不退还剩余时间的服务费用。

9.2 财务责任

FJCA 保证其具有维持其运作和履行其责任的财务能力。它应该有能力承担对订户、依赖方等造成的责任风险。

9.3 业务信息保密

9.3.1 保密信息范围

保密的业务信息包括但不限于以下方面：

- a) 在双方披露时标明为保密(或有类似标记)的；
- b) 在保密情况下由双方披露的或知悉的；
- c) 双方根据合理的商业判断应理解为保密数据和信息的；
- d) 以其他书面或有形形式确认为保密信息的；
- e) 或从上述信息中衍生出的信息。

对于 FJCA 来说，保密信息包括但不限于以下方面：

- a) 最终用户的私人签名密钥都是保密的；
- b) 保存在审计记录中的信息；
- c) 年度审计结果也同样视为保密；
- d) 除非有法律要求，由 FJCA 掌握的，除作为证书、CRL、认证策略被清楚发布之外的个人和公司的信息需要保密。

FJCA 不保存任何证书应用系统的交易信息。

除非法律明文规定，FJCA 没有义务公布或透露订户数字证书以外的信息。

9.3.2 不属于保密的信息

与证书有关的申请流程、申请需要的手续、申请操作指南等信息是公开的。

FJCA 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 FJCA 目录服务等方式向外公布。FJCA 在其目录服务器中公布证书的吊销信息，供网上查询。

9.3.3 保护保密信息责任

a) 各方有保护自己和其他人员或单位的机密信息的并保证不泄露给第三方的责任。不将机密数据和信息(也不会促使或允许他人将机密数据和 信息)用于协议项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;在披露当时,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。

b) 当 FJCA 在任何法律、法规或规章的要求下,或在法院等执法或司法部门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,FJCA 应 按照要求,向执法部门公布相关的保密信息,FJCA 无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

9.4 个人隐私保密

9.4.1 隐私保密方案

除非证书申请人主动提供,FJCA 保证不会截取任何证书申请人的资料。

FJCA 应保护证书申请人所提供的,证明其身份的资料。FJCA 应采取必要的安全措施防止证书申请人资料被遗失、盗用与篡改。

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 FJCA 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

当 FJCA 在任何法律、法规或规章的要求下，或在法院等执法或司法部门的要求下必须提供证书申请人的特定资料或隐私信息时，FJCA 按照法律、法规或规章的要求或法院等执法或司法部门的要求，向执法部门公布相关信息，FJCA 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处理。

9.5 知识产权

除非额外声明，FJCA 享有并保留对证书以及 FJCA 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。FJCA 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。

按本《电子认证业务规则》的规定，所有由 FJCA 签发的证书和提供的软

件中使用、体现和相关的一切版权、商标和其他知识产权均属于 FJCA 所有，这些知识产权包括所有相关的文件和使用手册。注册机构应征得 FJCA 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。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

FJCA 在提供电子认证服务活动过程中的承诺如下：

- a) FJCA 遵守《中华人民共和国电子签名法》及相关法律的规定，接受信息产业部的领导，对签发的数字证书承担相应的法律责任。
- b) FJCA 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。
- c) 除非已通过 FJCA 证书库发出了 FJCA 的私钥被破坏或被盗的通知，FJCA 保证其私钥是安全的。
- d) FJCA 签发给订户的证书符合 FJCA 的 CPS 的所有实质性要求。
- e) FJCA 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。
- f) FJCA 将及时吊销证书。
- g) FJCA 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。
- h) 证书公开发布后，FJCA 向证书依赖方证明，除未经验证的订户信息外，证书中的其他订户信息都是准确的。

9.6.2 注册机构的陈述与担保

FJCA 的注册机构在参与电子认证服务过程中的承诺如下：

- a) 提供给证书订户的注册过程完全符合 FJCA 的 CPS 的所有实质性要求。
- b) 在 FJCA 生成证书时，不会因为注册机构的失误而导致证书中的信息与证书申请人的信息不一致。
- c) 注册机构将按 CPS 的规定，及时向 FJCA 提交证书申请、吊销、更新等

服务请求。

9.6.3 订户的陈述与担保

订户一旦接受 FJCA 签发的证书，就被视为向 FJCA、注册机构及信赖证书的有关当事人做出以下承诺：

- a) 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。
- b) 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 FJCA 或注册机构检查和核实。
- c) 订户应当妥善保管私钥，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。
- d) 私钥为订户本身访问和使用，订户对使用私钥的行为负责。
- e) 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 FJCA 和注册机构，申请采取吊销等处理措施。
- f) 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 FJCA 吊销其证书。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉本《电子认证业务规则》的条款以及和订户数字证书相关的证书政策，并确保本身的证书用于申请时预定的目的。

依赖方在信赖订户的数字证书前，必须采取合理步骤，查证订户数字证书及数字签名的有效性。

所有依赖方必须承认，他们对证书的信赖行为就表明他们承认了解本《电子认证业务规则》的有关条款。

9.6.5 其他参与者的陈述与担保

其他参与者必须熟悉本《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。

其他参与者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。

所有其他参与者必须承认，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。

9.7 赔偿与担保免责

9.7.1 用户申请 FJCA 赔偿

FJCA 的赔偿责任范围：

- a) 证书信息与订户提交的信息资料不一致，导致订户损失。
- b) 因 FJCA 原因，致使订户无法正常验证证书状态，导致订户利益受损。

9.7.2 FJCA 申请用户赔偿

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 FJCA 和注册机构产生损失，订户和依赖方应承担赔偿责任。

订户接受证书就表示同意在以下情况下承担赔偿责任。

- a) 未向 FJCA 提供真实、完整和准确的信息，而导致 FJCA 或有关各方损失。
- b) 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。
- c) 在知悉证书密钥已经失密或者可能失密时，未及时告知 FJCA，并终止使用该证书，而导致 FJCA 或有关各方损失。
- d) 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。
- e) 证书的非法使用，即违反 FJCA 对证书使用的规定，造成了 FJCA 或有关各方的利益受到损失。

9.7.3 赔偿限额

FJCA对所有当事人的合计赔偿责任，不能超过如下所述的封顶赔偿金额。

- 1、个人类证书，不超过人民币2,000元
- 2、组织机构类证书，不超过人民币10,000元

所有相关当事人在接受及履行本《电子认证业务规则》的过程中，均已知悉并了解上述赔偿限额的法律意义，且不持异议。

9.7.4 责任免除

有下列情况之一的，应当免除 FJCA 之责任。

- a) 如果证书申请人故意或无意地提供了不完整、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 FJCA 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，FJCA 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。
- b) FJCA 不承担任何其他未经授权的人或组织以 FJCA 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。
- c) FJCA 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。
- d) FJCA 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。
- e) FJCA 和注册机构不是证书持有人或依赖方的代理人、受托人、管理人或其他代表。FJCA 和证书持有人之间的关系以及 FJCA 和依赖方之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 FJCA 承担信托责任。
- f) 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 § 9.14.4。
- g) 因 FJCA 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；（3）黑客攻击；（4）设备或网络故障。

h) FJCA 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。

所有相关当事人在接受及履行本《电子认证业务规则》的过程中，均已知悉并了解上述责任免除的法律意义，且不持异议。

9.8 有效期限与终止

9.8.1 有效期限

本《电子认证业务规则》自发布之日起正式生效，文档中将详细注明版本号、发布日期和生效日期，当新版本生效时，旧版本将自动失效。

由于必要原因，FJCA 在获得国家主管部门的批准后，可以宣布提前终止本《电子认证业务规则》的有效期。

9.8.2 终止

当新版本《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。

当 FJCA 中止业务时，FJCA 《电子认证业务规则》终止。当证书到期或吊销后，订户协议即终止。根证书有效使用期终止，对应的订户协议终止。

9.8.3 效力的终止与保留

《电子认证业务规则》中涉及的审计、保密信息、隐私保护、知识产权等方面，以及赔偿的有限责任条款，在本《电子认证业务规则》终止后继续有效。

9.9 对参与者的个别通告与沟通

任何主体对本《电子认证业务规则》中提到的服务、规范、操作等有疑问，或者希望提出修改意见，均可以书面形式，提交 FJCA。FJCA 经过研究，如认为

确有必要的，可以单独进行交流和沟通。

9.10 修订

9.10.1 修订程序

经FJCA运营安全管理小组授权组建的CPS编写小组每年至少审查一次CPS，确保其符合国家法律法规和主管部门的要求，符合认证业务开展的实际需要。

修订完成后，FJCA 运营安全管理小组进行审批，审批通过后将在 FJCA 的网站(<http://www.fjca.com.cn>)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。

9.10.2 通告机制和期限

本《电子认证业务规则》在 FJCA 的网站(<http://www.fjca.com.cn>)上发布。

版本更新时，最新版本的《电子认证业务规则》在 FJCA 的网站发布，对具体个人不做另行通知。

9.10.3 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》。

9.11 争议处理

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

- a) 当事人首先通知 FJCA，根据本《电子认证业务规则》中的规定，明确责任方；
- b) 由 FJCA 相关部门负责与当事人协调；
- c) 若协调失败，可以通过仲裁或司法途径解决；

- d) 任何因与 FJCA 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 FJCA 工商注册所在地的人民法院管辖。

9.12 管辖法律

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

9.13 与适用法律的符合性

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

9.14 一般条款

9.14.1 完整协议

本《电子认证业务规则》将替代先前的、与主题相关的书面或口头解释。

9.14.2 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。

9.14.3 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。

9.14.4 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，FJCA 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。

9.15 其他条款

FJCA 对本《电子认证业务规则》拥有最终解释权。