福建省数字安全证书管理有限公司
电子认证业务规则

版本 2.2.2

发布日期：2018 年 5月 1日

生效日期：2018 年 6月 1日

福建省数字安全证书管理有限公司

版权声明

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：福建省福州市晋安区秀山路 63-12 号

邮政编码：350003

联系电话：0591-968806

传　　真：0591-87816483

电子邮件：CPS@fjca.com.cn

目　录

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国家密码管理局《电子认证服务管理办法》的要求，依据《电子政务电子认证服务业务规则规范(征求意见稿)》制定，并报国家密码管理局备案。

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。FJCA 采用支持 SM2 密码算法电子认证系统，是全国第一家支持 SM2 椭圆曲线密码算法的认证机构。2013 年 1 月 FJCA 电子认证系统正式加入国家 SM2 信任源根 CA。

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《电子认证业务规则》，目前版本号为 V2.2.2，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、国家密码管理局电子认证服务管理办法和电子政务电子认证服务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---安全策略委员会。

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”负责编写。

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：福建省福州市晋安区秀山路 63-12 号

邮　　编：350003

电话号码：0591-968806

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》由安全策略委员会制定并执行。

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”提交安全策略委员会，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之内向国家密码管理局和国家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国家密码管理局的相关规定。

1.6 定义和缩写

下列定义适用于本《电子认证业务规则》：

1、电子认证服务机构（CA）

提供电子认证服务的认证机构

2、注册机构（RA）

接受公钥证书的申请、注销和查验申请材料的机构。

3、证书策略（CP）

一个指定的规则集合，它指出证书对于具有普通安全需求的一个特定团体和（或）具体应用类的适用性。

4、电子认证业务规则（CPS）

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。

5、证书吊销列表（CRL）

一个已标识的列表，它指定了一套证书发布者认为无效的证书。除了普通CRL外，还定义了一些特殊的CRL类型用于覆盖特殊领域的CRL。也称为证书黑名单列表。

6、在线证书状态协议（OCSP）

OCSP是一个请求/应答模式的协议，通过该协议可以获得当前证书的（吊销）状态，而无需查询CRL。在对证书状态的实时性要求较高的场合，适用于使用OCSP来查询当前证书状态。

7、电子签名认证证书（签名证书）

由证书认证机构签名的保护公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

8、电子签名人（证书持有者、订户）

拥有或持有电子认证服务机构签发的有效证书的个人、组织或实体。

9、电子签名依赖方（证书使用者、依赖方）

依赖于证书真实性的实体。依赖方可以是也可以不是一个证书持有者。

10、SM2密码算法（SM2算法）

一种椭圆曲线非对称密码算法，密钥长度为256比特，密码安全性更高、运算速度更快。

11、公开密钥基础设施（PKI）

用公钥密码技术建立的普遍适用的基础设施，为用户提供证书管理和密钥管理安全服务。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、加解密、完整性和不可否认性服务。

12、公钥(电子签名验证数据)

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、目录服务或其他公共目录中，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。

13、 私钥(电子签名制作数据)

私钥是经由数字运算产生的密钥，将电子签名与电子签名人可靠地联系起来的字符、编码等等组成数据。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。

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

1. 《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。
2. 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。
3. FJCA 的 CRL 每 4 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

每张数字证书包括有主体，目的是标识该证书由谁持有，这些主体的命名方法采用的 X.501 的甄别名检查方式 DN 通常包含以下部分或其部分 C 国家 S 所在省市等行政 L 地址 O 组织 OU 组织下的部门或分支 CN 主体名称 E 电子邮件 不同证书类型的 DN 的取值和编排方式有所不同，并且所有证书设计命名的内容都进过严格审核

各类数字证书 CN 的取值方式 ：

编号	证书类型	CN 取值方式

1	个人证书	个人姓名（与身份证明文件上标明的 主体名称（与机构有效证件上标明的 一致）
2	机构证书	机构名称（与机构有效证件上标明的 一致）
3	设备证书	域名、IP 地址或其他实体标识，与盖章 申请上标明的一致

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.501 DN 是 C=CN 命名空间下的 X.501 目录唯一名字。

属性	值
国家	CN
通用名	域名（服务器证书）或组织机构名（机构身份证书）或个人姓名（个人证书）或其他
机构	证书订户所在的机构名称或不填
机构部门	可以包含以下一个或多个内容，订户的组织机构 部门一个引用依赖方协议的申明，改依赖方协议 明确了使用证书的条款，版权通过描述证书类型的文字
城市	订户所在城市
省份	订户所在省份或不用
电子邮件	订户的电子邮件地址或不用

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。必须反映用户的真实身份，具有实际意义，并与法律不冲突。

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。认证申请人不得在其认证申请中使用会侵犯他人知识产权或商标专用权的名称。然而，FJCA 不会核查在认证申请中所出现的名称的认证申请人是否拥有该知识产权或商标专用权，亦不会仲裁，调解，或解决有关任何因网域名称，商标名称，服务标章所有权所引起争议，当此类争议出现时，FJCA 将依照先申请先使用的原则，并有权在认为有必要时驳回或挂起相关证书申请直到争议解决，且不需对任何证书申请人负法律责任。

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。

1、识别营业执照

（1）审查营业执照上的用户名与申请的用户名是否一致。

（2）看所提供的执照字迹是否完整，清晰，由当地工商行政机关颁发，并有颁发登记机关的公章。

（3）新版营业执照的鉴别方法：

A、登录国家工商总局官网，进入“国家企业信用信息公示系统”进行查询，复核申请用户所提供的营业执照内容。

B、《企业法人营业执照》、《营业执照》分为正本和副本，具有同等法律效力。

C、营业执照的内容主要包括：企业名称、统一社会信用代码、企业住所、法定代表人、注册资本、企业类型、经营范围、营业期限、成立日期、登记机关、发证日期等。

D、营业执照上面有一个二维码，在线扫码能获得详细信息。

E、统一社会信用代码是一组长度为 18 位的用于法人和其他组织身份识别的代码。规定统一社会信用代码用 18 位的阿拉伯数字或大写英文字母表示，由登记管理部门代码（1 位）、机构类别代码（1 位）、登记管理机关行政区划码（6 位）、主体标识码（组织机构代码）（9 位）和校验码（1 位）5 个部分组成。

F）看执照上的有效年限。要求都在使用期内，严防过期失效。

2、识别组织机构代码证

（1）审查组织机构代码证是否由中华人民共和国国家质量监督检验检疫

总局统一印制。

（2）审查代码证上是否盖有中华人民共和国国家质量监督检验检疫总局鉴章（大红印）。

（3）颁发《中华人民共和国组织机构代码证》为各级质量技术监督局

（4）看代码证上是否采用了专用水印纸。

（5）看代码证上是否印刷了防涂改底纹。

（6）审查组织机构代码证的原件与复印件是否一致。

（7）审查机构代码证是否盖有质量技术监督局的年审印章。

3、识别税务登记证

（1）核对税务登记证的注册号与组织机构代码号的后 9 位是否一致。

（2）审查税务登记证与申请单位名称是否一致。

（3）审查税务登记证是否由当地国家税务局和地方税务局合并颁发，并加盖当地国家税务局和地方税务局税务登记专用章（二个印）。

（4）提供副本的，在税务登记证副本上有没有企业的电脑编码。

4、识别社保登记证

（1）审查社保登记证原件与相要求提供的复印件是否一致，申请表填写的单位名称与社保登记证的用户名是否一致。

（2）社保登记证是否经过年审，有效期是否有效。

（3）社保登记证是否盖有当地社会劳动保险公司颁发。

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 保留根据最新国家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。

FJCA《电子认证业务规则》规定，个人身份的鉴别可以使用以下有效的身份证件：居民身份证、居民户口簿、护照、军官证、警官证、士兵证、士官证、文职干部证、港澳台居民身份证、外国人永久居留证。

1、第二代身份证

（1）在一般的光线下，平视第二代身份证表面时，表面上的物理防伪膜是无色透明的；适当上下倾斜“二代身份证”，便会观察到证件的左上方有一个变色的长城图案，呈橙绿色；用左眼和用右眼分别观察，身份证上的长城图案的颜色将呈不同颜色；将身份证旋转 90 度（垂直方向），观察到的长城图案呈蓝紫色。

（2）新版身份证：侧光验看在正面的照片正下方处有 “中国 CHINA”。

（3）真身份证公章上的所有文字和姓名、性别、出生、地址、编号等文字的横笔均为平直笔划，如“市、安”，横笔的收笔处无三角。假身份证则不同，如“市、安”，横笔的收笔处有三角。

（4）真身份证反面国徽中顶部，大五角星上角正指一处有麦穗相对形成的“ ”形缺口。假身份证“缺口”与真身份证“缺口”有所不同，即使形状相同，但两侧麦穗形状模糊不清，导致“缺口”不成形态。

2、居民户口簿

（1）封面是深褐色皮革底色，正中是国徽，金字“居民户口簿”“中华人民共和国公安部制”并有英译文。

（2）第一页左下角红章“XX 省公安厅户口专用”，其中红章的五星正上方一个角刚好印在“公”和“安”的空隙间，并且登高、对称。

（3）左上角一般标有地段号，新版一般有 8 位数字。

（4）右下角红章“XX 市公安局户口专用 XX 派出所”，其中“专”字为特殊处理的___，竖线与最后一点行程直线，印章为手工盖的，外围为双圆环状，并且内外圆环间的空隙极小，很均匀，且线条一般不是很圆滑。

（5）登记内容为：户别、户主姓名、户号、住址、签发时间。

（6）页与页的缝线是机器缝的线眼很均匀统一，每厘米的宽度最少有两个线眼。

（7）第二页始：右下角印章同第一页。

（8）常住人口登记卡，所有登记内容均为黑色打印提，非手写体。

（9）同一时间、同一派出所签发的，每页的承办人应该是同一人签发。

（10)迁徙情况栏如是没发生的,则应该是空着的,没内容,不应该写“无”。

3、护照

（1）护照的封面：护照封面顶部通常是国家名称，中间是各个国家的国徽标识，下面是护照的种类。如果要简单区分一本护照是哪个国家的，最好从国徽标志区分。

（2）打开护照后，会看到护照的资料页、备注页以及护照的内页（签证页）。资料页是客户的详细资料，备注页用来记录换发记录以及变更自己的姓名的记录。内页用来张贴签证，加盖验讫章。可以看到护照资料页可以分为上中下三个区域组成，顶部区域可以看到护照的种类（P），签发国的代码（CHN），右侧是护照号码。中部是旅客主要的资料，包括姓名、性别、国籍、出生日期、出生地点、签发日期、有效日期、签发机关和本人的照片。底部是机读区域（与中部内容是对应一致的）。注意一点：顶部的国家代码是签发国家的代码，而底部的国家代码指的是旅客的国籍。

（3）护照号码的格式：因私普通护照号码格式有:14/15+7 位，,G+8 位数；因公普通的是:P.+7 位数。公务的是：S.+7 位数或者 S+8 位数，以 D 开头的是外交护照 D=diplomatic。

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

互操作可能是交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各自认证策略的电子认证服务机构之间建立相互信任关系，使双方的用户可以实现互相认证。

FJCA 可根据业务需要，在遵循《电子认证业务规则》的各项控制要求的

基础上，与 FJCA 证书服务体系中未涉及的其他电子认证服务机构建立交叉认证关系。

如果国家法律法规对此有规定，FJCA 将严格予以执行。

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

FJCA 通过 RA 受理实体的证书申请，证书申请的实体可以是任何个人，机构或其它客观存在的实体，其本人或机构的合法授权代表或实体拥有者都可以为该实体提交证书申请，证书申请人提交的信息必须真实，否则后果由证书申请人承担。FJCA 为机构的证书申请表格设置经办人栏，该经办人视为获得机构授权办理数字证书相关业务，包括接受数字证书。

申请人须清楚了解及同意订户协议的内容，特别是关于责任和担保的内容，并根据申请的证书类型提供真实，可靠，完整的身份资料，承担任何因提供虚假伪造信息所产生的法律责任。

FJCA 数字证书申请流程为：

1、证书申请人从网上下载打印或从 FJCA 所属 RA 获取相应实体种类的数字证书申请表格，按表格要求填好申请表并加盖公章。部分业务（如换证）也可以通过 FJCA 的在线服务系统提交申请信息。

2、开通应用服务可通过传真或邮件的方式受理。

3、按照本文 3.2 身份鉴别要求提交对应实体类型的证书申请表格及相关身份证明资料，到 FJCA 或其 RA 进行注册、身份审核和交费。

4.1.1 证书申请实体

证书申请实体包括具体独立法人资格的企业单位、事业单位、政府机构、社会团体等各类组织机构与个人用户。

4.1.2 证书申请过程与责任

证书申请人按照《电子认证业务规则》所规定的要求，通过在线方式或离线方式，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：用户要按照本《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，对用户所提供的证书申请信息与身份证明资料进行身份鉴别验证。

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 RA 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 RA 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 的注册机构对收到的材料进行确认，对资料填写齐全，公章正常，所附材料清晰，款项正常的情况下，将在 2 个工作日内处理证书申请；各 RA 注册机构在对资料填写齐全，公章正常，所附材料清晰，款项正常的情况下可现场受理证书申请。

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并生效。

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：

1. 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；
2. 邮政信函通知订户；
3. 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 构成接受证书的行为

下列行为被认为订户已经接受了证书：

1. 订户接受了包含有证书的介质；
2. 订户通过网络将证书下载或安装到本地存储介质，如本地计算机、USB Key、移动硬盘或其它移动存储介质；
3. 订户接受了获得证书的方式，并且没有提出反对证书或者证书中的内容。

4.4.2 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。

4.4.3 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和协议。订户接受到数字证书，

应妥善保存其证书对应的私钥，不得转让其使用的数字证书。

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。

对于签名证书其私钥可用于对信息的签名，在可能的情况下，签名证书及信任链上的证书（根证书除外）应同被签名信息一起提交给依赖方，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，证书持有应妥善保管其证书私钥。

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以下方面的内容：

1.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。

2.检验证书的有效期，确认该证书在有效期之内。

3.查询证书状态，确认该证书没有被注销。

4.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。

当依赖方接受到数字签名的信息后应该：

1).获得数字签名对应的证书及信任链

2).确认该签名对应的证书是依赖方信任的证书

3).检查证书是否有效

4).证书的用途使用与对应的签名

5).使用证书上的公钥验证签名信息。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。

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

4.6 证书更新

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 180 天，到 FJCA 授权的注册机构或在线更新系统申请更新证书。

证书更新的具体情形如下：

1. 证书有效期将要到期或已到期，证书需要继续使用。

2. 密钥对使用到期。

3. 订户或其授权代表提出证书的更新申请。

4. CA 的策略要求或相关法律法规引致其它原因。

5. 其他原因

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、机构及设备等各类证书的证书持有人。

4.6.3 证书更新请求的处理

处理证书更新请求可以采用两种方式：

第一种方式是在线更新。对于 FJCA 签发的个人、机构等证书订户，在获得 FJCA 授权后，自助进行在线证书更新操作，更新证书信息和有效期，获得新证书。

第二种方式是人工方式更新。适合所有证书更新情形，即订户或其授权代表提交证书更新申请表和身份证明材料，到 FJCA 或其 RA 进行证书更新，其身份鉴别方式和处理过程与本文组织机构身份的鉴别个人身份的鉴别要求相同。

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：

1. 通过面对面的方式，通知证书更新已完成，新证书已颁发；
2. 邮政信函通知订户；
3. 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

对于签发的任何最终用户证书，证书到期前 180 天系统将会自动提醒用户证书将到期，如果用户希望继续使用证书，订户可以申请证书密钥更新。证书密钥更新的情形如下：

1. 证书的有效期将要到期，证书更新；
2. 因私钥泄漏而吊销证书；

3.订户或其授权代表提出证书密钥的更新申请；

4.CA 的策略要求或相关法律法规引致其他原因；

4.7.2 请求证书密钥更新的实体

请求证书密钥更新的实体同 4.6.2。

4.7.3 证书密钥更新请求的处理

证书密钥更新请求的处理同 4.6.3。

4.7.4 颁发新证书对订户的通告

颁发新证书给订户的通告同 4.6.4。

4.7.5 构成接受密钥更新证书的行为

正式接受密钥更新证书的行为同 4.6.5。

4.7.6 电子认证服务机构对密钥更新证书的发布

FJCA 对密钥更新证书的发布同 4.6.6。

4.7.7 电子认证服务机构对其他实体的通告

FJCA 在颁发证书时对其他实体的通告同 4.6.7。

4.8 证书吊销

4.8.1 证书吊销的情形

1. 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。
2. 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。

4.8.2 请求证书吊销的实体

根据不同的情况，订户、FJCA、RA 注册机构可以请求吊销最终用户证书。

4.8.3 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。

1. 证书吊销的申请人到 FJCA 授权的注册机构书面填写《福建省数字证书综合业务申请表》，并注明吊销原因；
2. 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；
3. 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 4 小时内进入 CRL，向外界公布；
4. 强制吊销是指当 FJCA 或 FJCA 授权的 RA 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。

4.8.4 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。RA 应在收到吊销请求后立即吊销证书，没有宽限期，当最终订户发现数字证书私钥泄露或丢失，数字证书中的信息发生重大变更或用户不希望继续使用数字证书时，订户应当立即到 CA 注册机构申请吊销数字证书，吊销手续遵循 CA 的相关规定。用户应当承担所有在数字证书吊销之前使用数字证书而造成的后果。其他吊销原因的吊销请求必须在 48 小时内提出。

4.8.5 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,4 小时生效。FJCA 每日签发 6 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：

1. 版本号(version)
2. 签名算法标识符(signature)
3. 颁发者名称(issure)
4. 本次更新(this update)
5. 下次更新(next update)
6. 用户证书序列号/吊销日期(user certificate/revocation date)
7. CRL 条目扩展项(crl entry extensions)
8. CRL 扩展域(crl extensions)
9. 签名算法(signature algorithm)
10. 签名(signature value)

4.8.6 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：

1、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。

2、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。

4.8.7 CRL 的颁发频率

FJCA 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 4 小时自动发布最新 CRL，如遇特殊情况，人工发布最新 CRL。

4.8.8 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。

4.8.9 在线状态查询的可用性

FJCA 须提供证书状态的在线查询服务（OCSP），以供安全保障要求高的应用使用。

4.8.10 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，依赖方在信赖一个证书前必须通过证书状态在线查询检查该证书的状态。

4.8.11 吊销信息的其他发布形式

FJCA 提供 CRL、OCSP 的吊销信息发布，无其他形式。

4.8.12 密钥损害的特别要求

当订户发现、或有充足的理由发现其密钥遭受安全威胁时，应及时地提出证书吊销请求。

4.9 证书挂起

4.9.1 证书挂起的情形

当证书仍处于有效期，为了保留订户的证书使用权利，而不申请吊销该证书，当出现下列情况时，可以进行证书挂起：

1．证书订户要求暂停使用该证书一段时间；

2．订户未能履行与 FJCA 签订的协议中应尽的义务，但向 FJCA 提出申请并获得批准后；

3．除证书订户（或者其授权的委托代理人）外的其它实体，如电子认证服务机构及其授权的服务机构、法院、政府主管部门及其他公共权利部门，向 FJCA 提出挂起证书请求并获得批准。

4.9.2 请求证书挂起的实体

只有证书订户本人或者其授权的委托代理人，以及电子认证服务机构及其授权的服务机构、法院、政府主管部门及其他有关部门等，才有权力提出证书挂起的请求。

4.9.3 挂起请求的流程

订户在申请证书挂起时，由 FJCA 受理点根据申请变更的证书种类，发放相应的申请表，订户填写完后申请；受理点根据申请表进行证书挂起注册等制作工作。订户在申请办理电子认证证书挂起时，有责任在证书申请中提供准确有效的信息，提供相关的证明文件。 除证书订户以外的其它实体，如 FJCA 的授权机构、政府公共权力部门等，提出证书挂起请求，也需按规定填写申请表并提交证明材料。 FJCA 审核通过挂起请求后，应在一个工作日内办理挂起操作。

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。OCSP 发布点的地址：http://202.109.194.226:6080

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：

1. 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；

2. 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：

1. 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；
2. 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 、蓝牙 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。

1. 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。
2. 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

1. 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》
2. FJCA 机房位于福建省福州市晋安区秀山路 63-12 号三层 CA 机房，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，功能区域按低到高划分为不同的四个安全等级，为接入区，服务区，管理区和核心区。并采取了一定的隔离、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：

1.门禁系统：可控权限和时间的门禁系统控制各层门的进出。FJCA 的门禁系统有进出时间记录和超时报警提示。FJCA 设置指纹和智能卡双因素门禁系统来提高授权的安全性，并在进入管理区和核心区时才采用双人控制策略。工作人员需使用身份识别卡结合指纹双因素控制鉴定才能进出，进出每一道门应有时间纪录和信息提示。有业务需要的必须在授权的工作人员陪同下才可以进入相应限制区域活动。

2、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。

3、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。

4、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。FJCA 对监控记录的保存时间至少 3 个月，FJCA 的门禁系统有进出时间记录和超时报警提示，FJCA 定期对门禁记录进行整理归档，门禁进出时间记录的保存时间至少 1 年。

5.1.3 屏蔽机房

FJCA 设置屏蔽机房，进行电磁屏蔽，防止外部电磁场对系统设备的干扰，防止电磁信号泄露造成的信息泄露。主要将核心设备及系统存放在屏蔽机房。

FJCA 电磁屏蔽机房机构形式采用焊接式，由专业技术部门进行性能测试，测试性能指标符合国家相关标准。电磁屏蔽机房配件应采用滤波器、波导管、截止波导通风窗等屏蔽件，安装位置应便于检修；屏蔽门可分为旋转式和移动式，宜采用旋转式屏蔽门。所有进入电子屏蔽室的电源线缆应通过电源滤波器进行处理；所有进入电磁屏蔽室的信号电缆应通过信号滤波器处理；进出电磁屏蔽室的网路线宜采用光纤或屏蔽线，光纤不应带有金属加强芯。门禁系统电缆可采用 485 协议转换器控制，监控录像系统电缆使用光电转换信号的方式，消防控制系统电缆亦应采用信号转换，保证机房的屏蔽效果；屏蔽机房门禁管理必须采用双人、身份识别门禁卡加指纹鉴别的方式控制进出。宜使用安全侦

测系统，当人员撤出、机房门关闭同时，立即进行安全区域布防；能够及时识别、发现安全区人员异常活动；当发生人员异常活动时，应立即以声、光告警，并应能定位告警具体区域。具体设计如下：

1、设计依据

根据用户提出的具体要求，并对现场实地丈量，参照 GJBZ20219-94 标准进行设计。

2、构特点与用途

屏蔽机房从结构上区分为可拆卸和不可拆卸式两类，广泛用于抗干扰测试，保密等。

3、技术指标

本机房选用 JP-999A 型金属板组装贴焊式电磁屏蔽机房，实用于频带较宽场合的抗干扰。其屏蔽效能如下表：

	磁场			平面波	微波	
频段				50-1000MHZ	1-10GHZ	10-20GHZ
屏蔽 dB	55	70	90	100	100	80

4、外围设施

电源滤波：所有引入屏蔽机房的电源须经过滤波措施。本机房装有一套 DL-15 型滤波器，用户可根据需要增订或扩容。DL-15 型电源滤波器是采用 LC Л 型网络和吸收式微波滤波器的串联结构。微波滤波器是套插在波导管内，其内导体作为电源引线。整个滤波器是用特制的外壳加以屏蔽。

接地：屏蔽机房必须单独一点接地，接地电阻小于 2Ω，接地线一端连接顶板上的接地柱，另一端接大地（不可和电气接地及其他接地线混用）。用户

必须自备相应的专用接地线。

5、墙面、柱面

KM 中心加密机房及 CA 加密机房采用六面体钢板屏蔽，以保证这两个机房数据的保密性。其余机房区域全部采用彩钢板装饰，装饰板的宽度根据装饰效果而定，该板具有坚固耐用、光洁平整、防火无毒、隔音抗震、抗热耐冷、防腐蚀、抗污染、易于清洁等优点。对于机房的墙面来说较为适合，能够提高机房装饰效果，同时也能起到一定的屏蔽作用。

5.1.4 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。

各系统均采用 UPS 备用电源，保证不间断进行访问控制。FJCA 机房使用两台 20KVA 8 小时延时的台达 UPS 不间断电源，同时配备一台 150KW 发电机。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。空调系统使用独产空调。其组成包括空调、 通风管路。

FJCA 严格按照国家机房管理相关规定，并且定时对系统进行检查，确保其符合设备运行要求。

5.1.5 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。

5.1.6 火灾防护

火灾预防：

1. 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。
2. 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。
3. 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。
4. 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。
5. 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。
6. 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。
7. 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：

1. 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。

2. 手动方式：人员对钢瓶或药剂瓶直接开启操作。

3. 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。

5.1.7 介质存储

FJCA 的存储介质包括硬盘、软盘、磁带、光盘等各类软件运营数据和记录的各类介质，存储地点设有安全保护，防止诸如潮湿，磁力灾害以及人为可能造成的危害和破坏，同时记录介质的使用储存维修销毁事件等和公司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，进行监控并且只有授权人员才能进入。

5.1.8 防雷击和接地

FJCA 机房符合国家标准的防雷措施，具体如下：

设置综合地线系统；屏蔽机房必须设立保护地线，应经常检测接地电阻，确保人身、设备和运行的安全；应设置交流电源地线，交流供电应采用符合规范的三芯线，即相线、中线、地线。

计算机系统安全保护地电阻值、计算机系统防雷保护地电阻值必须符合国家标准。

1. 计算机系统的直流工作地

计算机以及一切微电子设备，大部分采用中、大规模集成电路，工作于较低的直流电压下，为使同一系统的计算机、微电子设备的工作通路具有同一“电位”参考点，将所有设备的“零”电位点接于一接地装置，它可以稳定电路的电位，防止外来干扰，这称为直流工作接地。

计算机直流工作接地电阻的大小、接法以及诸地之间的关系，应依不同计算机系统要求而定。一般要求该电阻不大于 1Ω，接地电阻越小越好。在条件许可的情况下，计算机机房设置独立的直流接地系统。接地引上线经铜过渡带，用 BV50 电缆引至机房配电室。

2. 交流工作地

交流工作地的作用是为确保人身安全和保障设备的安全。在计算机系统

的交流设备中其交流工作地的实施是将其中性点用绝缘导线串联起来接到配电柜的中线上，然后用接地母线将其接地。

交流工作地的接地电阻应不大于 4Ω 。

3. 安全保护地

安全保护地的作用为在绝缘被击穿时保护人身和设备的安全和在绝缘未被击穿时也有保护人身安全的作用。计算机机房内的安全保护地是将所有机柜的机壳，用数根绝缘导线串联起来，在用接地母线与大地相连。

安全保护地的接地电阻应不大于 4Ω 。

4. 计算机系统的防雷保护地

计算机系统的防雷接地其目的就是要避免雷电的发生，从而保护建筑物、计算机设备和人员的安全。为防止感应雷沿机房电源线进入，损坏机房内设备，在各配电柜进线处均设置德国进口菲尼克斯避雷器。防雷地阻小于 10Ω 。

5. 静电接地

在重要区域和工作人员经常走动的地方设置相对的抗高频干扰接地组。本机房在各功能间均设置相应的抗高频干扰接地组。

6. 弱电设备的直流接地

弱电设备的直流电源大多有自己的特定技术要求，一般都是随主机设备成套供应的，也有由设计单位按要求配套采购的，特别是交流供电用的稳压器和不间断电源。

弱电设备的直流接地是旁路电气杂音干扰和稳定电压基准的必要措施，如程控交换机 48V 直流电源正极工作接地和电子计算机的逻辑接地。

弱电设备一般都要求有自己的隔离型直流接地装置，因此在直流接地体共用基础接地网的情况下必须保证直流接地线在整个范围都是绝缘的，但是对于上引至机房的直流地线，为防止雷击，应设置雷击均压火花放电间隙。直流接地装置的总接地箱宜设置在主楼地下室的适当地方，并就近用不少于两根的 50 平方毫米绝缘铜线连接到基础接地网上。从总直流接地箱可分别引出三根 25 平方毫米绝缘铜线至程按交换机机房、电子计算机房和其它要求直流接地的机房的分直流接地箱，再用 16 平方毫米的绝缘铜线引到各自的系统设备机架上。

以上除直流逻辑接地采用独立的直流接地系统外，其余接地系统均接入

大楼综合接地。

考虑到 FJCA 的具体情况。经过现场勘察，在 FJCA 机房所在地做了一套直流逻辑地。

5.1.9 静电防护

FJCA 机房采用防静电地板和建材装饰机房；应控制机房温、湿度在合适范围内，防止静电产生；机房应良好接地。在重要区域和工作人员经常走动的地方设置相对的抗高频干扰接地组。本机房在各功能间均设置相应的抗高频干扰接地组。

5.1.10 新风系统设计

为了使计算机操作人员在较封闭的机房内工作能有舒适感，这样就需要在使用空调的同时不断补充新风，补充新风的另一作用还在于可保持机房内正压，提高机房洁净度。

根据机房设计规范及贵机房现场实际情况，要求机房内每人每小时补充 40m3 的新风量。通过新风管道将过滤过的新风送至电源室的吊顶上，从地板下送入机房，达到补充新鲜空气的作用，新风经过滤后，其含尘量也满足了机房的要求，新风管道采用镀锌板制作，在新风机出口处安装防火阀和调节阀，防火阀可接消防信号实现消防联动，调节阀可用于调节新风量。

5.1.11 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。

5.1.12 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 或其授权的注册机构、依赖方等组织中与密钥和证书生命周期管理操作

有关的工作人员，都是可信角色，必须由可信人员担任。

FJCA 明确规定 CA 关键职能的职位，主要包括但不限于以下部分：

1. 安全策略委员会主任
2. 可信人员管理员
3. 安全管理员
4. 物理环境安全管理员
5. 密钥管理员
6. 运行维护管理员
7. CA 系统管理员
8. 系统维护管理员
9. 数据库管理员
10. 网络管理员
11. 运行审计管理员
12. 鉴别与验证员
13. 信息录入员
14. 信息审核员
15. 档案管理员
16. 其他。

FJCA 根据《电子认证服务机构从业人员岗位技能规范》等标准规范与本 CPS 的要求，制订其授权的证书服务机构（RA 等）的管理规范，规范证书服务机构和服务系统的管理人员、操作人员的操作。在与此相关的软件设计中，充分考虑安全的限制与约束。FJCA 对授权的证书服务机构的责任进行合理划分，并通过系统和技术实现以及管理的责任义务上进行保证。

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，对于重要的系统操作与维护，FJCA 通常会安排一人进行操作，一人进行监督记录。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

为保证系统安全，遵循可信角色分离的原则，即 FJCA 的可信角色由不同的人担任。

对于证书服务的受理，必须通过业务办理人员（或录入人员）、鉴别验证人员、业务执行人员等多个角色进行才能完成。

至少两个人以上才能使用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。

FJCA 在系统遇到紧急情况需要联合抢修时，至少派遣 1 名 FJCA 工作人员在场。抢修人员需在 FJCA 工作人员陪同下，执行许可的操作。所有的操作、修改都保留记录。

非 FJCA 工作人员因基础装修、消防、强（弱）电故障等情形，需要进入机房实施修理时，必须经 FJCA 安全策略委员会主任同意后，首先对修理者的身份进行验证，然后由 FJCA 指定的工作人员始终陪同和监督，完成约定部位的修理。

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：

1. 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。

2. 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。

3. 新入职的员工必须经过一个月的观察期，观察期通过后才可独立上岗现场考核、日常观察、情景考验等方式对其考察。

4. 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。之后 CA 不定期进行可信人员背景调查，以便能够持续验证人员的可信程度。CA 确立流程管理规则，据此 CA 员工受到合同和章程的约束，不许泄露 CA 认证服务体系的敏感信息，所有的员工与 FJCA 签订保密协议。

5. 可信人员调续期间或员工离职日起 2 年内仍然不得从事与 FJCA 相类似

CA 电子认证业务规则劳动合同关系的工作。

5.3.3 培训要求

FJCA 对所有人员按照其岗位和角色安排不同的培训。培训内容主要包括：

1. FJCA 的安全原则和机制、岗位职责；
2. 电子认证系统相关软、硬件的安装与维护；
3. 电子认证系统的操作与使用；
4. FJCA 的业务管理相关的流程、标准与规范；
5. FJCA 的运行管理相关的规章、制度与管理办法；
6. 国家电子认证相关的法律法规与政策；
7. 其他必要的培训。

对于运营人员，有关 CA 的相关知识与技能，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，为不断提高员工业务素质和综合能力同时根据 CA 策略调整，系统更新升级或功能增加等情况，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，以更快更好适应新的变化。

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

CA 员工所有涉及到业务操作安全的操作均有记录，由 CA 系统管理员或安

全审计员审查，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，中止该员工进入 CA 证书认证体系各系统，当事人的证书和操作权限及时冻结或注销，所做的未授权操作将立即被注销失效，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，依法追究相应责任包括内部处分，辞退，解雇等，涉及犯罪的将送司法机关处理。

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：

1. 人员档案进行备案管理；
2. 签署保密协议；
3. 必须接受 FJCA 组织的相关知识与安全规范培训；
4. 由 FJCA 派专人监督或者陪同从事相关在工作。

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，主要包括（但不限于）：

1. 认证系统相关软、硬件的操作手册，例如，认证系统操作手册、密码设备用户手册、目录服务器安装配置说明文件等；
2. 电子认证业务规则与相关的协议和规范；
3. 系统运行与维护相关的流程、管理办法，例如，机房设备管理办法；
4. 电子认证服务相关的宣传资料；
5. 内部操作文件，例如，灾难备份和恢复方案；
6. 其他文档。

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 定期对日志进行审查，并对审查日志的行为进行备案。每年进行的审查不少于 2 次。

5.4.3 审计日志的保存期限

审计日志的数据库记录保存3个月，纸质文件保存五年。异常情况记录和报表的保存至少10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 将审计日志存储到光盘中，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

CA的审计日志分手工采集和自动采集两种方式，自动采集的主要是电子日志通过CA系统（包括各子系统）网络设备，各计算平台产生并记录，手工采集的主要是纸质日志，通过操作或出入人员的手工记录产生。

审计日志收集系统涉及：

- 证书管理系统；
- 证书签发系统；
- 证书目录系统；
- 远程通信系统；
- 证书受理系统；
- 访问控制系统；
- 网站、数据库安全管理系统；
- 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信息安全管理委员会，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至少每年要对物理场地、运营管理、人事管理进行运营评估。每年委托第三方检测机构对电子认证系统及密钥管理系统进行安全脆弱性评估，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；
6. 人员变更记录等保存 5 年；
7. 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。FJCA 电子认证系统 RSA 根证书有效期至 2020 年。SM2 根证书有效期至 2033 年。

1. FJCA 根密钥由加密机产生，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。

2. 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。

3. 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。

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。

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《电子认证业务规则》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《电子认证业务规则》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。

FJCA建立了系统数据备份系统，在物理场地或系统数据出现重大灾难时，能够根据需要尽快恢复其业务。

5.8 电子认证服务机构或注册机构的终止

因各种原因，CA所属注册机构需要暂停或终止证书运营情况下，并按照相关法律法规的要求进行档案和证书的存档。

注册机构应在暂停或终止业务前90个工作日书面通知CA并通告其所办理证书的订户，CA将作出妥善的安排，由其它注册机构或新设注册机构承接其业务尽量减少对CA及证书订户的影响。

注册机构业务终止之日起60个工作内，所有业务档案资料将无条件移交给FJCA或FJCA指定的承接注册机构。

FJCA 采用以下措施终止业务：

1、起草 FJCA 终止业务声明；

2、停止认证中心所有业务；

3、处理加密密钥；

4、处理和存档敏感文件；

5、清除主机硬件；

6、管理 FJCA 系统管理员和安全官员；

7、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 、蓝牙 KEY 或智能 IC 卡）生成，加密密钥对由 KMC 生成。签名密钥对由用户端产生，证书申请可使用福建省国家密码管理局认可的，CA 数字证书签发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 CA 无法复制签名密钥对。

根密钥对及其下级 CA 密钥的生成，是在预设定的程序下，由至少 3 名密钥管理员及 1 名监督人员参与下产生，并对每个环节进行记录和签名。用户签名密钥对在客户端产生，存储在介质中的签名密钥不可导出，CA 具有严密且安全的控制措施。

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 CA 的私钥只能保存在 CA 控制的密码设备和采取秘密分割的备份介质中，禁止向外传递.保证传递中间环节加密私钥不泄露

订户的签名私钥在订户的电子密钥或其它密码设备生成后随其事务通过离线方式传递到订户，订户面对面的交递或采取密码信封保护方式发送给订户

在最终订户生成自己的密钥对的情况下，不需要将私钥传给订户，如果认证机构或注册机构在硬件中未最终订户生成密钥对，那么它应该通过安全的采用了防篡改技术的方式将这些密钥分给最终订户。

6.1.3 公钥传送给证书签发机构

订户的公钥采用证书签发请求格式或其它专门的安全格式通过安全通道经注册机构传递传递给 CA 完成证书签发，订户证书签发后其公钥再随证书由

CA 发布到 CA 的证书库，证书依赖方可以从 CA 证书库下载该公钥，CA 的公钥或其直接生成证书的公钥，则直接由 CA 签发证书后随证书发布到 CA 证书库供订户和依赖方下载.在此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 电子认证系统支持 RSA 算法和 SM2 算法。RSA 非对称密钥对的模长是 1024 比特，SM2 非对称密钥对的长度是 256 比特。

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，FJCA 将会完全遵从相关标准。

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

用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。

所有密钥的使用，均必须遵循本《电子认证业务规则》的规范。

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

CA 使用国家密码主管部门许可的密码产品其密码模块符合国家规定的

标准要求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。

CA 使用国家密码管理部门认可的密码设备产生 CA 密钥对，CA 也使用密码硬件设备来存储密钥对

在密码硬件设备的初始化，上线销毁等生命周期内 CA 有相应的策略来保障硬件密码设备的安全

CA 密码设备遵循多人在场，多人控制的原则

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，即采取三选二方式，将私钥的管理权限分散到 3 张管理员卡中，只有其中二至三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。加密私钥由国家密码管理部门 KMC 备份，备份数据以密文形式保存。

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 使用无锡江南信息安全工程技术中心 SJY42-C，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：

1. 通信接口：符合国际 ITU Ethernet RJ45 标准；
2. 带宽控制：10M/100M 自适应，充分满足突发业务需要；
3. 并发容量：可支持同时并发 100 个的独立安全处理容量；
4. 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；
5. 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；
6. 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。

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电子签名，私钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期限以外，直到私钥受到损害或密钥对存在被破解的风险，如加密算法被破解。当私钥受到损害或密钥对存在被破解的风险后，签名证书的公钥在技术上仍然可以用于验证数字签名，但这种验证在法律上不一定是有效的。

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

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

另外无论是订户证书还是 CA 证书，有效期到期前，在保证安全的情况下，允许证书进行更新而密钥对不变。但是密钥对不能无限期使用。

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。

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：

1. 专人负责设备的领取和保管，做好设备的领用、进出库和报废登记。

2. 对设备定期进行检查、清洁和保养维护。
3. 制定设备维修计划，建立满足正常运转最低要求的易损坏备件库。
4. 对设备进行维修时，必须记录维修的对象、故障原因、排除方法、主要维修过程及与维修有关的情况等。
5. 设备维修时，必须有派专人在场监督。

6.5.2 计算机安全评估

FJCA 已取得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：0011。

FJCA 取得工信部颁发的电子认证服务许可证，证书编号：ECP35010511016。

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 的信息安全管理，严格遵循国家密码管理局等主管部门的有关运行规范和 FJCA 的安全管理策略进行操作。

FJCA 的使用具有严格的控制措施，所有和系统都经过严格的测试验证后才进行使用。任何修改和升级均记录在案并进行版本控制、功能测试和记录。FJCA 还对认证系统进行定期和不定期的检查与测试。

FJCA 采取严格的管理体系来控制和监视系统的配置，以防止未授权的修改。

所有设备从采购到上线前，均进行安全性检查。密码设备的采购与安装，

在更加严格的安全控制机构下，进行检验、安装与验收。

对废旧设备进行处理时，必须确认其是否有影响认证业务安全性的信息存在。

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国家密码管理局的鉴定与安全性审查，使用基于标准的强化安全通信协议以确保通信数据的安全；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 RFC5280 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：

- 颁发机构密钥标识符 Authority Key Identifier
- 主体密钥标识符 Subject Key Identifier
- 密钥用法 Key Usage
- 扩展密钥用途 Extended Key Usage
- 私有密钥使用期 Private Key Usage Period
- 主体可选替换名称 Subject Alternative Name
- 基本限制 Basic Constraints
- 证书撤销列表分发点 CRL Distribution Points

私有扩展项可支持以下类型：

- 个人身份证号码 Identify Card Number
- 企业工商注册号 IC Registration Number
- 企业组织机构代码 Organization Code
- 企业税号 Taxation Number
- 证书唯一码 Certificate Unique Code
- 个人社会保险号 Social Security Number
- 统一社会信用代码 Uniform Social Credit Code

7.1.3 算法对象标识符

1. RSA 证书使用 SHA1WithRSAEncryption 算法， 算法 OID 为 1.2.840.113549.1.1.5；

2. SM2 证书使用 SM3withSM2 算法，算法标识 OID 为 1.2.156.10197.1.501。

7.1.4 名称形式

FJCA 数字证书中的主体 Subject 的 X.501 DN 是 C=CN 命名空间下的

X.501 目录唯一名字，各属性的编码一律使用 UTF8String。

主体 Subject 的 X.501 DN 支持多级 O 和 OU，其格式如下：

CN=××

OU=××;

OU=××;

O=××

O=××

C=CN;

- C（Country）应为 CN，表示中国；
- O（Organization）中的内容分为 2 种：

1. 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；
2. 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；

- OU（Organization Unit）应为证书主体或者证书主体所属单位的名称全称；
- CN（Common Name）中的内容分为 4 种：

1. 个人证书中应为证书主体的姓名；
2. 单位机构证书中应为证书主体单位的标准简称；
3. 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；
4. 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；
5. 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《电子认证业务规则》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，评估合格后方可以正式运营。

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《电子认证业务规则》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。

自行的内部审计由信息安全管理委员会负责组织实施，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：

- 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审计人员或审计评估机构，且在业界享有良好的声誉。
- 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。
- 具备检查系统运行性能的专业技术。

8.3 审计或评估人员与 CA 的关系

CA 内部审计人员要求与被审计对象无责任关系，为 CA 雇员。

CA 内部风险评估的负责人要求与被评估对象无责任关系，可以是 CA 雇员，也可以是非 CA 雇员。

外部审计或评估人员应为与 CA 无任何除审计或评估之外的业务，财务往来或其他足以影响评估客观性的厉害关系。

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：

- 是否制订和公布电子认证业务规则；
- 是否按照本《电子认证业务规则》来制订相关的操作规范和操作流程；
- 是否接受对所有流程和操作的审计；
- 是否按照本《电子认证业务规则》及相关操作规范和操作流程开展业务；
- 是否符合本《电子认证业务规则》及与之相关的授权协议；
- 服务的完整性；

- 物理与环境安全控制；
- 系统与网络安全控制；
- 人员的安全控制；
- 建筑设施的安全控制；
- 软硬件设备的存储介质的安全控制；
- 系统开发和维护的安全控制；
- 灾难恢复和备份系统的管理；
- 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. 国家密码管理局在完成审查后，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

数字证书的收费根据证书实际应用的需要，收费价目表如下：

收费项目		年服务费	备注
机构类型	机构法人证书	200 元/份	用于证明单位合法身份，可作为单位网上合法身份的证明，一证多用。

序号	收费项目		年服务费	备注
1	机构类型	机构业务专用证书	200 元/份	用于证明单位在网上办理某一项特定业务的合法身份，一证一用。
		机构岗位专用证书	150 元/份	用于证明单位内部个人岗位的合法身份，代表单位行使岗位职能时使用。
		安全电子邮件证书	60 元/份	安全电子邮件传送或向需要客户验证的 WEB 服务器表明身份。
		企业代码签名证书	1000 元/份	证明软件开发商的合法身份，用于对其发布的软件代码进行签名时使用。
2	个人类型	自然人证书	130 元/份	证明个人用户的合法身份，一证多用，用于个人网上办理各种业务。
		安全电子邮件证书	10 元/份	安全电子邮件传送或向需要客户验证的 WEB 服务器表明身份
		个人代码签名证书	130 元/份	证明软件开发者的合法身份，用于对其发布的 软件代码进行签名时使用。
3	设备类型	设备证书	3000 元/份	用于表明服务器合法身份
4	可信站点		1 万元/户	为正规网站提供安全认证服务，申请了认证服务的网站可以得到一个来自 FJCA 的信任站点的认证签章，把信任站点认证签章显示于网站上。互联网用户通过点击认证签章可以即时获得可信第三方提供的信任信息，确认所访问的网站不是冒充或诈骗网站，可以提高用户对网站的信任度。

序号	收费项目	费用	备注
1	电子签名验证报告	580 元/份	验证数据签名 10 条以内
2	电子签名验证报告	980 元/份	验证数据签名 10 条以上至 100 条以内
3	电子签名验证报告	另行计算	验证数据签名 100 条以上
4	证书信息变更（机构）	30 元/份	

5	证书信息变更（自然人）	15 元/份	
6	证书密钥恢复	50 元/份	
7	证书注销（机构）	10 元/份	
8	证书注销（自然人）	5 元/份	
9	证书挂起	10 元/份	
10	邮寄费	20 元/份	

硬件介质费：150 元／个 （用于办理新证和证书遗失或证书损坏需补证时）

说明：证书服务费按年收取。服务期满后未续费的，服务终止。

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 保持足够的财力维持其业务运作和履行应负的责任财务能力，CA 接受国家电子认证服务主管部门对 CA 财务状况的检查。当因不遵守操作规程而造成的 RA 身份审核不当，因 CA 密钥泄露而造成的订户或依赖方不应承受的损失，CA 根据本《电子认证业务规则》相关法规进行赔付。

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：

1. 在双方披露时标明为保密(或有类似标记)的；

2. 在保密情况下由双方披露的或知悉的；
3. 双方根据合理的商业判断应理解为保密数据和信息的；
4. 以其他书面或有形形式确认为保密信息的；
5. 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：

1. 最终用户的私人签名密钥都是保密的；
2. 保存在审计记录中的信息；
3. 年度审计结果也同样视为保密；
4. 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 保护保密信息的责任

1. 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。

2. 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

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

CA 尊重所有的用户和他们的隐私，并制定隐私保护策略，所有相关人员包括 CA 及其 RA 的工作人员订户等必须严格遵守相应的规章制度，以符合国家法规要求，任何人选择使用 CA 的任何服务，那么就表示已经同意接受 CA 有关隐私保护的声明。

9.4.2 作为隐私处理的信息

CA 在管理和使用订户申请，注册证书时提供的相关信息时，除了证书已经包括的信息外，该订户的基本信息和身份认证资料，非经订户同意或者法律法规及权力部门的合法要求，绝对不会任意对外公开。

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

CA，任何订户，关联体以及从认证业务相关的参与方等，都有义务按照本 CPS 的规定，承担相应的保护保密信息的责任。

当 CA 在任何法律法规或者法院通过合法程序的要求下，或者信息所有者书面授权的情况下，CA 可以向特定对象相关的隐私信息，CA 无效为此承担任何责任，而且这种被披露不被视为违反了隐私保护义务。如果这种隐私披露导致了任何损失，CA 对此不应承担任何责任，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

CA 在其认证业务内使用所获得任何订户信息，只用于订户身份识别，管理和服务订户的目的，在使用这些信息时，无论是否涉及到隐私，CA 都没有告知订户的义务，也无需得到订户的同意。

CA 在任何法律法规或者法院通过合法程序的要求下，或者信息所有者书面授权的情况下向特定对象披露隐私信息时，也没有告知订户的义务，并且不需得到订户的同意。

CA 与其授权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，在法律允许的情况下，事前需告知订户，并得到用户端的同意和书面签章授权。

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

CA 自身拥有的知识产权声明：

除非额外声明，FJCA 享有并保留对证书以及 CA 提供的全部软件的一切知识产权，其它任何人未经 CA 的书面同意，不得以任何方式，任何途径进行复制，存储，使用或传播，包括但不限于所有权，名称权和利益分享权等，CA 关联实体采用的证书服务软件系统，选择采取的形式、方法、时间、过程和模型，以保证系统以便保证系统的兼容和互通。

CA 发行的证书及其状态信息，以及 CA 提供的软件，系统，文档中使用，

体现和设计到的一切版权，商标和其他知识产权均属于 CA 提供软件，系统，文档中使用，体现和涉及到的一切版权，商标和其他知识产权属于 CA，这些知识产权包括所有相关的文件，CPS 规范文档和使用手册等

在没有 CA 预先书面同意的情况下，订户不能在任何证书到期，作废，或终止的期间或之后，使用或接受任何 CA 使用的名称，商标，交易形式或可能与之相混淆的名称，商标，交易形式或商务称号。

CA 使用其他方知识产权的声明：

CA 使用其服务系统中使用的软硬件设备，辅助设施和相关操作手册，其知识产权为相关供应商所有，CA 保证都是合法的拥有相应权利

订户或证书申请人声明并保证其交付给 CA 使用的网络域名，IP 地址，主体名称及所有其它证书申请书的资料不得在任何管辖区域内干预或侵犯第三人的商标，服务标志，公司名称或其它知识产权等权利，而且不用于非法目的，包括侵害，干扰协议或预期的商业利益，不公平竞争，损害他人信誉及干扰或误导他人。

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：

1. 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。
2. 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。
3. 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。
4. FJCA 签发给订户的证书符合 FJCA《电子认证业务规则》的所有实质性要求。
5. 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。

6. FJCA 将及时吊销证书。
7. 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。
8. 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：

1. 提供给证书订户的注册过程完全符合 FJCA《电子认证业务规则》的所有实质性要求。
2. 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。
3. 注册机构将按本《电子认证业务规则》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

订户一旦接受公司签发的证书，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：

1. 订户需熟悉本《电子认证业务规则》的条款和与其证书相关的证书政策，
2. 还需遵守证书持有人证书使用方面的有关限制。
3. 订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，可供 FJCA 或注册机构检查和核实。
4. 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。
5. 私钥为订户本身访问和使用，订户对使用私钥的行为负责。
6. 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。
7. 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：

1. 证书信息与订户提交的信息资料不一致，导致订户损失。
2. 因 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。

1. 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。

2. 未能保护订户的私钥，或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用时。
3. 在知悉证书密钥已经失密或者可能失密时，未及时告知 FJCA，并终止使用该证书，而导致 FJCA 或有关各方损失。
4. 订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或 多个数字签名后理所当然地相信这些表述，订户必须对这种行为的后果负责。
5. 证书的非法使用，即违反 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。

3. 设备类证书，不超过20,000 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

CA 在以下三种情况下免除责任

1 不可抗力

在不可抗力情况下，CA 免除责任。

2 免责条款

免责条款是指当事人在合同中约定的免除将来可能发生的违约责任的条款，免责条款不得违反法律的强制性规定和社会公共利益。

3 债权人过错

如果合约不履行或在不完全履行是由对方即债权人的过错造成的，不履行或者不完全履行的一方免除违约责任，在电子认证服务合同中也存在因债权人过

错而免责的情况，包括但不限于以下内容

申请者故意或无意提供不完整，不可靠或已过期的，包括但不限于 ，篡改，虚假的信息，而其又根据政策的流程提供了必须的审核文件由此得到了 CA 签发的数字证书；

订户或依赖方没有使用可信赖系统进行证书操作；

订户在 CA 允许的目的范围之外使用或证书使用不当；

以上未尽事宜，依照中华人民共和国现行法律，法规执行。

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安全策略委员会授权组建的电子认证业务规则编写小组每年至少审查一次《电子认证业务规则》，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，信息安全管理委员会进行审批，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：

1. 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；
2. 由公司相关部门负责与当事人协调；
3. 若协调失败，可以通过仲裁或司法途径解决；
4. 任何因与 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。