福建省数字安全证书管理有限公司
证书策略

版本 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

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：0591-87856110

电子邮件：CP@fjca.com.cn

目 录

1 简介

本文系证书策略(CP)，福建省数字安全证书管理有限公司，是经国家工信部批准的福建省地区性从事数字证书制作、颁发和管理的权威机构。

FJCA 作为“数字福建”公用信息平台的安全基础设施为我省电子商务、电子政务和网上作业保驾护航，对国民经济信息化和电子商务发展过程起到积极的作用。

FJCA 的发展目标是在为网络交易和作业的主体提供信任和安全服务的同时不断的完善和进步，最终成为国内首屈一指的电子商务认证中心。

证书策略（CP，CertificationPolicy）是关于认证机构（CA,Certification Authority）制订的策略，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。本证书策略的适用范围为 FJCA 发放的所有证书。在 FJCA 证书策略中，它为批准、签发、管理、使用、吊销、更新证书和相关的可信服务制定商务、法律和技术上的规范。这些规范是 FJCA 证书的标准，它应用于保护 FJCA 证书的完整性和安全性。

本文档由 FJCA 安全策略委员会负责编写、修改、更新、及评述整理。同时负责监督对 CP 的要求遵循情况。

1.1 概述

FJCA 作为一个证书服务机构（CA），在本 CP 的约束下生成根证书和子 CA 证书，签发订户证书。证书注册机构（RA）是 FJCA 内鉴别证书请求的实体，FJCA 本身同时也是一个 RA，其他组织、企业等通过与 FJCA 签署协议，也可以作为 FJCA 的 RA，鉴别其相关用户的证书请求。基于不同的类型和应用范围，作为证书持有人的订户可以使用证书进行网络站点安全保护、代码签名、邮件签名、数据/文件签名及验证签名、数据/文件加解密、身份认证、等不同的应用。依赖方依照本 CP 中关于依赖方的义务要求，决定是否信任一张证书。FJCA 的电子认证业务规则（CPS）接受本 CP 的约束，详细阐述了 FJCA 作为电子认证服务机构提供的证书、如何提供证书以及相应的管理、操作和保障措施。所有 FJCA 证书的订户及依赖方必须参照本 CP 及相关 CPS 的规定，决定对证书的使用和信任。

1.1.1 第 1 类证书

个人身份证书，包括身份证书，在网络通讯中标示证书持有者的个人身份，可以用于个人网上进行合同签订、订单、支付信息等活动中表明身份。

1.1.2 第 2 类证书

单位证书，包括：机构身份证书、单位代码签名证书。为用户提供的身份保证必须确认：订户组织机构确实存在，该组织机构授权证书申请，并且订户代表提交证书申请要获得授权审核。机构身份证书是以单位或机构作为可信实体对象，发放的单位身份证书”。

1.1.3 第 3 类证书

服务器证书，包括：服务器身份证书和应用服务器证书，它们主要用于提供网络信息认证确认访问者真实身份。

1.2 文档名称与标示

文档名称是《FJCA 证书策略》，目前版本号为 V2.2，在 FJCA 网站发布，网站地址为 http://www.fjca.com.cn

1.3 PKI 的参与者

1.3.1 电子认证服务机构（CA）

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（Registration Authority）

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 受理点（Registration Authority Terminal,RAT）

经过 FJCA 审查，FJCA 授权特定单位或实体，负责办理和审批数字证书申请数字证书申请手续、过程和要求，必须与 FJCA 正在实施的数字证书策略（CP）以及 FJCA 的 CA 受理点授权协议书相一致。受理点负责向 FJCA 授权的注册机构提供证书申请实体的信息，包括申请实体的名称、可以表明身份的证件号码和联系方法（通信地址、电子邮件信箱、电话等），并为申请实体提供技术支持。

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，使用其他公司证书的公钥的实体。

1.3.5 证书种类和订户

从电子认证服务机构接收证书的实体。在电子签名应用中，订户即为电子签名人，指证书和证书相关服务的使用者。FJCA 中有三种类型证书：1 类证书是仅签发给个人最终订户的个人身份证书。2 类单位身份证书只可以签发给一个组织机构。3 类服务器证书有些可以签发给个人，有些可以签发给组织机构，还有些可以签发给组织机构的服务器。因此，3 类证书所对应的组织机构将作为注册机构。

1.3.6 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 合适的证书应用

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证书策略规范的要求，FJCA制定本《证书策略》，并指定专门的机构---安全策略委员会。负责制定、维护和解释本CP。本《证书策略》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《证书策略》在 FJCA 网站发布，对具体个人不另行通知。

联系人：福建省数字安全证书管理有限公司系统运行部

地址：福建省福州市晋安区秀山路 63-12 号

电话：0591-968806

邮编：350003

传真：0591-87856110

电子邮址： fjkefu@fjca.com.cn

1.5.3 决定 CP 符合策略的机构

FJCA安全策略委员会决定本CP的符合性和可用性。FJCA安全策略委员会作为最高策略管理机构，是批准和决定FJCA或者其它某个CA的CPS是否符合本CP的机构。

1.5.4 CP 批准程序

FJCA的CP由系统运行部起草拟定后，提交法律顾问审阅审核。如果因需要对CP进行修改，由运行部修改建议报告，由安全策略委员会评审通过后在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备案。

1.5.5 CP 发布

在CP修改审批之后，由运行部在FJCA网站 http://www.fjca.com.cn上公布变更后的CP。对本CP所做的修改，将于FJCA发布之日起立即生效。所进行的修改将取代以往CP各版本中的任何冲突和指定条款。

根据《中华人民共和国电子签名法》、《电子认证服务管理办法》的规定，FJCA在公布 CP 后向工业和信息化部备案。

1.6 定义和缩写

下列定义适用于本《证书策略》：

1. 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。

2. 证书策略(CP) Certification Practice

是指本证书策略文档，是一个有关 CTN 业务策略的主要
说明。

3. 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。

4. 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)。

5. 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。

6. 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。

7. 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。

8. 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。

9. 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 信息库

FJCA 的 http://www.fjca.com.cn 网站，电子认证系统的证书服务站点，LDAP、CRL、OCSP 服务及注册机构的证书服务站点构成 FJCA 认证信息发布的信息库。本《证书策略》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 认证信息的发布时间或频率

1. 《证书策略》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 CP、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 识别与鉴别

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。，实体名字可以是姓名、组织机构名、域名、IP 地址等。

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 解释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《证书策略》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。

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《证书策略》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

FJCA 暂未提供互操作服务。

3.3 密钥更新请求的标识与鉴别

订户证书到期后，订户需对原有证书进行更新。在更新时产生一个新的密钥对代替过期的密钥对，称之为“密钥更新”。在密钥更新时，证书的 DN 未改变。

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

吊销请求可来自于订户，也可来自 CA 或 RA。在申请吊销时，订户递交与申请证书时相同的身份材料进行身份鉴别。递交的方式可以为， 如传真、 申请书等向认证机构提交请求，认证机构或注册中心通过相应的通讯方式与订户联系，确认要吊销的证书是订户本人。 审核后为订户吊销证书。

4 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 注册过程与责任

证书申请人按照本《证书策略》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《证书策略》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《证书策略》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《证书策略》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《证书策略》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 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 证书签发中发证机构和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 电子认证服务机构和发证机构对订户的通告

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。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：

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。

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

证书更新是指在是在不改变证书中的公钥和其他任何证书包含的信息的情况下，为订户签发一张新证书。证书更新时无需再提交证书注册信息，订户提交能够识别原证书的足够信息，如订户甄别名、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。

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：

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：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《证书策略》3.2.2 和 3.2.3。

4.6.4 颁发更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 构成接受更正证书的行为

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密钥更新证书的发布

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

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 处理证书密钥更新请求

证书密钥更新请求的处理同 4.6.3。

4.7.4 通知订户新证书的签发

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 证书变更

4.8.1 证书变更的情形

1. 证书的主体内容发生改变；
2. 证书的 E-mail 地址发生改变；
3. 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、机构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《证书策略》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：

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。

4.8.5 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

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。

4.9.2 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 请求吊销的流程

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《证书吊销申请表》，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 24 小时内进入 CRL，向外界公布；
4. 强制吊销是指当 FJCA 或 FJCA 授权的注册机构确认用户违反本《证书策略》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，每 4 小时签发一次 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：

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. f) 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)

4.9.6 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：

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。

4.9.7 证书 CRL 发布频率

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 4 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

证书从它被吊销到被发布到 CRL 上的滞后时间不超过 24 小时。

4.9.9 在线的吊销/状态查询的可用性

FJCA 提供在线的吊销/状态查询，该服务 7X24 小时可用。

4.9.10 在线的吊销查询要求

依赖方在信赖一张证书前须确定证书的状态， 查询方式为检查 CRL 或 OCSP。

4.9.11 吊销信息的其他发布形式

除 CRL 与 OCSP 之外，尚无其它发布形式。

4.9.12 对密钥遭受安全威胁的特别处理要求

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。

4.10 证书状态服务

4.10.1 操作特征

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 服务的可用性

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 可选功能

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。

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. 证书、证书吊销列表和在线证书状态协议

5.1 证书

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

5.1.1 版本号

X.509 V3。

5.1.2 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 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

5.1.3 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。

5.1.4 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：

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：

  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；
- 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；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。

5.2 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。

5.2.1 版本号

X.509 V2。

5.2.2 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

5.3 在线证书状态协议

5.3.1 版本号

使用 OCSP 版本 1（OCSP v1）。

5.3.2 OCSP 扩展项

不使用 OCSP 扩展项。

6. 法律责任和其他业务条款

6.1 费用

6.1.1 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，可以对证书价格进行适当调整。

6.1.2 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。

6.1.3 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。

6.1.4 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。

6.1.5 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。

6.2 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。

6.3 业务信息保密

6.3.1 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。

6.3.2 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。

6.3.3 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《证书策略》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。

6.4 个人隐私保密

6.4.1 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。

6.4.2 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。

6.4.3 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。

6.4.4 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。

6.4.5 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。

6.4.6 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。

6.4.7 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。

6.5 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《证书策略》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。

6.6 陈述与担保

6.6.1 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 的 CP 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，
9. 证书中的其他订户信息都是准确的。

6.6.2 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 的 CP 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 CP 的规定，及时向 FJCA 提交证书申请、吊销、更新等服务请求。

6.6.3 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：

1. 订户需熟悉本《证书策略》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。

6.6.4 依赖方的陈述与担保

依赖方必须熟悉本《证书策略》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《证书策略》的有关条款。

6.6.5 其他参与者的陈述与担保

其他参与者必须熟悉本《证书策略》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《证书策略》的有关条款。

6.7 赔偿与担保免责

6.7.1 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。

6.7.2 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。

6.7.3 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《证书策略》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。

6.7.4 责任免除

有下列情况之一的，应当免除 FJCA 之责任。

1. 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。
2. 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
3. 散布的不可信赖的信息所引起的法律责任。
4. 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。

5. 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。
6. 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 和证书持有人间的关系以及 FJCA 和依赖方间的关 系并不是代理人和委托者的关系。证书持有人和依赖方都没有权利以合 同形式或其他方法让 FJCA 承担信托责任。
7. 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§6.14.4。
8. 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。
9. FJCA 已谨慎地遵循了国家法律、法规规定的数字证书认证证书策略，而仍有损失产生的。

所有相关当事人在接受及履行本《证书策略》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。

6.8 有效期限与终止

6.8.1 有效期限

本《证书策略》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《证书策略》的有效期。

6.8.2 终止

当新版本《证书策略》正式发布生效时，旧版本的《证书策略》自动终止。

当 FJCA 中止业务时，FJCA《证书策略》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。

6.8.3 效力的终止与保留

《证书策略》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《证书策略》终止后继续有效。

6.9 对参与者的个别通告与沟通

任何主体对本《证书策略》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。

6.10 修订

6.10.1 修订程序

经信息安全管理委员会授权组建的CP编写小组每年至少审查一次CP，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《证书策略》。

《证书策略》将进行严格的版本控制。

6.10.2 通告机制和期限

本《证书策略》在 FJCA 的网站(http://www.fjca.com.cn)上发布。

版本更新时，最新版本的《证书策略》在 FJCA 的网站发布，对具体个人不做另行通知。

6.10.3 必须修改证书策略的情形

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《证书策略》。

6.11 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《证书策略》中的规定，明确责任方；
2. 由 FJCA 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《证书策略》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。

6.12 管辖法律

本《证书策略》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。

6.13 与适用法律的符合性

无论在任何情况下，本《证书策略》的执行、解释、翻译和有效性均适用中华人民共和国的法律。

6.14 一般条款

6.14.1 完整协议

本《证书策略》将替代先前的、与主题相关的书面或口头解释。

6.14.2 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。

6.14.3 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。

6.14.4 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。

6.15 其他条款

FJCA 对本《证书策略》拥有最终解释权。