JXCA C P S

电子认证业务规则

版本 V2.0

生效日期：2007 年 7 月 10 日

目　　录

1 概括性描述

1.1 概述

江西省数字证书有限公司（以下简称JXCA）是为电子签名提供第三方认证服务的电子认证服务机构。JXCA的电子认证业务规则详细阐述了JXCA在提供认证服务过程中，制定并对外公布有关数字证书的业务类型、证书制作、证书管理、认证作业及信息安全保障的实施规程。包括：证书的申请、审核、签发、撤销、更新、变更、挂失、冻结等操作流程，以及信息公开的要求等内容。对于JXCA所提供的认证服务过程的责任范围，本业务规则也给予了明确的规定。

1.2 文档名称与标识

本文为 JXCA 电子认证业务规则（ CPS ），在 JXCA 网站发布，JXCA 网址：http://www.jxca.org.cn。

JXCA 是江西省数字证书有限公司（JiangXi Certification Authority）的英文简称。

JXCA 的标识为：

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

JXCA 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。JXCA 通过给从事电子交易活动的各方主体颁发数字证书、提供证书验证服务等手段而成为电子认证活动的参与主体。

1.3.2 注册机构

JXCA 的数字证书注册机构是经 JXCA 正式授权后的业务分支机构，包括证书注册审核（RA）中心、证书本地受理（LRA）点等。注册机构是为 JXCA 的证书申请者建立注册过程的实体。

1.3.3 订户

在电子签名应用中，订户即是电子签名人，是接收本机构签发证书的实体

1.3.4 依赖方

JXCA的证书依赖方是指基于对JXCA提供电子认证活动中电子签名的信赖而从事有关活动的实体。该实体可以是，也可以不是JXCA的一个证书订户。

1.3.5 其它参与者

其他参与者是指为 JXCA 的电子认证活动提供相关服务的其他实体。

1.4 证书应用

1.4.1 适合的证书应用

JXCA 签发的数字证书常见的应用范围包括电子商务、电子政务、其他社会信息化应用。

目前 JXCA 可以签发的证书种类有以下四类：

1、个人数字证书

2、单位数字证书

3、服务器证书

4、代码签名证书

1.4.2 限制的证书应用

JXCA 签发的数字证书禁止的应用范围包括：

1、根据《中华人民共和国电子签名法》第三条规定，民事活动中的合同或

者其他文件、单证等文书，当事人可以约定使用或者不使用电子签名、数据电文。当事人约定使用电子签名、数据电文的文书，不得仅因为其采用电子签名、数据电文的形式而否定其法律效力。前款规定不适用下列文书：

（一）涉及婚姻、收养、继承等人身关系的；

（二）涉及土地、房屋等不动产权益转让的；

（三）涉及停止供水、供热、供气、供电等公用事业服务的；

（四）法律、行政法规规定的不适用电子文书的其他情形。

2、JXCA 与订户约定的证书禁止应用范围。

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 的制订、更新、发布等事宜，其管理机构为 JXCA 运营安全管理小组。

1.5.2 联系人

CPS 维护组　　电话：0791-6212680　EMAIL：jxca@jxca.org.cn

1.5.3 决定 CPS 符合策略的机构

JXCA 运营安全管理小组拥有对 JXCA CPS 的决策权和审批权。

1.5.4 CPS 批准程序

批准流程是：

（1） CPS 编写组编写 CPS。

（2） CPS 编写完成后提交 JXCA 各部门修改。

（3） 修改后的 CPS 递交运营安全管理小组审查。

（4） 运营安全管理小组审查通过后，CPS 正式对外发行。

1.6 定义和缩写

1.6.1 术语定义一览表

电子签名认证证书	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、资格即其他有关信息的电子文件。
数字证书	使用数字签名作为识别签名人身份和表明签名人认可签名数据的一种电子签名认证证书。
电子签名	具有识别签名人身份和表明签名人认可签名数据的功能的技术手段。
数字签名	通过使用非对称密码加密系统对电子记录进行加密、解密变换来实现的一种电子签名。
电子签名人	是指持有电子签名制作数据并以本人身份或者以其所代表的名义实施电子签名的人
电子签名依赖方	是指基于对电子签名认证证书或者电子签名的信赖而从事有关活动的人。
私钥（电子签名制作数据）	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。
公钥（电子签名验证数据）	是指订户验证电子签名的数据。

1.6.2 缩略语及其含义一览表

JXCA	Jiang Xi Certificate Authority	江西省数字证书认证中心
CA	Certificate Authority	电子认证服务机构
KMC	Key Management Center	密钥管理中心
RA	Registration Authority	注册审核服务机构
LRA	Local Registration Authority	本地注册受理点
LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
CPS	Certification Practice Statement	电子认证业务规则
CRL	Certificate Rovoke List	证书撤消列表
CSR	Certificate Signing Request	证书签名请求
OCSP	Online Certificate Status Protocol	在线证书状态协议
PIN	Personal Indentification Number	证书个人识别码
PKCS	Public KEY Cryptography Standards	公共密钥密码标准
PKI	Public Key Infrastructure	公共密钥基础设施
X.509		国际电信同盟认证体系的证书标准

2 信息发布与信息管理

2.1 认证信息的发布

JXCA 电子认证信息库包括以下内容：CPS、证书、CRL，该信息库的运营实体为 JXCA 机构本身。JXCA 的职责是使发布的认证信息及时可靠。

2.2 发布的时间或频率

JXCA 通过网站方式公布本机构制定的 CPS。对于因认证业务需要进行的 CPS 的不定期变更，JXCA 也将通过文档版本升级的形式，以原有公布方式予以及时发布。JXCA 的 CRL 可以实时发布和定期发布。

2.3 信息库访问控制

对于以网站方式公布的 CPS 认证信息，JXCA 允许任何公众进行查询和访问。证书和 CRL 通过 LDAP 方式予以发布，同时提供 OCSP 在线验证方式。JXCA 采取授权和安全审计等安全管理手段，保证了证书、CRL 等认证信息库的登陆和访问控制。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

JXCA 签发的数字证书格式中，遵循国际电信联盟（ITU）提出的 X.509 版本和 Internet 工程任务组（IETF）颁布的 ORC3280 规定，对证书持有人唯一标识符包含在证书的“DN”项中。该项标识了本证书所提到的最终实体的唯一身份标识。

3.1.2 对名称意义化的要求

DN 项中的名称标识符具有一定的代表性意义，可为个人订户的身份证号码、机构订户的组织机构代码等。

3.1.3 订户的匿名或伪名

本 CPS 规定，JXCA 的订户在进行数字证书申请时不能够使用匿名或伪名。

3.1.4 理解不同名称形式的规则

DN 的具体内容依次由 CN、E、OU、O、L、S、C 几部分组成。其中 CN 用来表示用户名，E 表示电子邮箱，OU 表示证件号码，O 表示名称，L 表示地址，S 表示省，C 表示国家。

3.1.5 名称的唯一性

JXCA 数字证书的主体名称项具有唯一性。当同一订户申请多张证书时，遵循先申请者优先使用DN项,后申请者在DN项增加附加识别信息予以区别的原则。

3.1.6 商标的识别、鉴别和角色

JXCA 不接受使用商标作为名称标识符的订户申请。

3.2 初始身份验证

3.2.1 证明拥有私钥的方法

通过证书请求中包含的数字签名来证明用户持有与注册公钥对应的私钥。在JXCA 体系中，用户私钥（private key）在用户端生成，用户的证书请求信息中包含用私钥进行的数字签名，CA 用对应的公钥可以验证这个签名。JXCA 要求用户妥善保管自己的私钥，因此，用户视作其私钥的唯一持有者。

3.2.2 组织机构身份的鉴别

JXCA 在接到组织机构类订户的证书申请后，向该订户签发证书前，必须对该组织机构身份进行查验和鉴别。鉴别要求如下：

1、组织机构的授权办理人携带本人身份证原件及复印、机构工商营业执照登记证及复印件、组织机构代码证原件及复印件亲自到证书申请现场。

2、核对办理人身份证、机构工商营业执照登记证、组织机构代码证原件与复印件是否一致。

3、核对办理人身份证、机构工商营业执照登记证、组织机构代码证信息与申请表相应信息是否一致。

4、确认组织机构接受 JXCA“数字证书用户责任书”中的各项条款。

5、检查该订户提交申请材料的完整性。

3.2.3 个人身份的鉴别

JXCA 在接到个人类订户的证书申请后，向该订户签发证书前，必须对该证书申请者的个人身份进行查验和鉴别。鉴别要求如下：

1、证书申请个人携带本人身份证原件及复印件亲自到证书申请现场。通过面对面核实方式确认该订户的真实身份。

2、核对申请者身份证原件与复印件是否一致。

3、核对申请者身份证原件信息与申请表相应信息是否一致。

4、确认该申请者接受 JXCA“数字证书用户责任书”中的各项条款。

5、检查该订户提交申请材料的完整性。

3.2.4 设备身份的鉴别

JXCA 在接到订户的设备证书申请后，向该订户签发设备证书前，必须对该证书申请者及申请设备的身份进行查验和鉴别。鉴别要求如下：

1、订户为组织机构的身份鉴别按照本 CPS 3.2.2 节描述执行。订户为个人的身份鉴别按照 3.2.3 节描述执行。

2、核查证书订户与设备的责任关系证明材料与订户的身份证明材料是否一致。

3.2.5 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。

3.2.6 授权确认

个人订户或机构订户在 JXCA 的数字证书申请表上加盖单位有效公章后，则证明本机构对个人或办理人进行 JXCA 证书申请的授权确认。

3.2.7 互操作准则

经过 JXCA 的合法授权后，注册机构可对订户的证书申请执行以上的初始身份确认方法。

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

JXCA 在接到注册机构或订户的常规密钥更新请求后，将使用该订户证书中的当前有效密钥对对包含新密钥的密钥更新请求进行签名，作为对常规密钥更新的标识与鉴别。

3.3.2 吊销后密钥更新的标识与鉴别

证书被吊销后，对密钥更新的鉴别将按照该订户初始身份的验证过程进行。

3.4 吊销请求的的标识与鉴别

JXCA 对证书吊销请求的鉴别要求包括：

1、订户本人申请吊销证书；

2、订户没有履行双方合同规定的义务。

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

JXCA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CPS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。JXCA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CPS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

JXCA 或授权的注册机构按照本 CPS 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 .身份标识与识别

4.2.2 证书申请批准和拒绝

JXCA或授权的注册机构根据本CPS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CPS所规定的身份鉴别流程且鉴证结果为合格，JXCA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，JXCA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

JXCA授权的注册机构将做出合理努力来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JXCA的管理要求。

4.3 证书签发

4.3.1 证书签发中注册机构和电子认证服务机构的行为

JXCA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。

4.3.2 电子认证服务机构和注册机构对订户的通告

JXCA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；注册机构把数字证书直接提交给订户，来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JXCA认为其他安全可行的方式通知订户。

4.4 证书接受

4.4.1 构成接受证书的行为

数字证书签发完成后，注册机构将数字证书当面或寄送给证书申请人。证书申请人从获得数字证书起，就被视为同意接受证书。

4.4.2 电子认证服务机构对证书的发布

订户接受证书后，JXCA 在其规定的时间内将该订户证书发布到 JXCA 的目

录服务系统。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JXCA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

用户需要妥善保管自己的私钥和证书，不将其用于不适合的证书用途（在1.4.2 节定义），也不可在证书已过期或被吊销的情况下继续使用证书和密钥。

4.5.2 依赖方公钥和证书的使用

依赖方有义务妥善保存用户的公钥和证书，不将其用于不适合的证书用途，使用前有责任根据 CPS 的规定检查证书的有效性。

4.6 证书更新

为保证证书及其密钥对的安全有效，JXCA 为签发的证书设置有效期，一般为一年。这也是为了保证证书用户的权利。证书用户必须在证书有效期到期前一个月内，到 JXCA 授权的发证机构申请更新证书。更新证书时发证机构根据用户的要求决定新证书是否使用原证书密钥。出于安全考虑建议证书用户更新证书时更新密钥。

4.6.1 证书更新的情形

证书更新的原因

- 证书的使用期限将要到期；
- 其他。

证书更新指 JXCA 在不修改证书中的订户相关公开身份信息的情况下重新签发一张证书。

4.6.2 请求证书更新的实体

请求证书更新的实体为证书订户。

4.6.3 证书更新请求的处理

1、订户可到证书申请的注册机构进行证书更新申请。

2、证书订户填写“证书更新申请表”表单。

3、注册机构对申请订户的身份进行查验与鉴别，鉴别要求同本 CPS 中 3.2.2、3.2.3 节描述。

JXCA 注册机构先注销旧证书后，再为证书订户发放新证书。

4.6.4 颁发新证书时对订户的通告

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；

4.6.5 构成接受更新证书的行为

见 4.4.1 构成接受证书的行为。

4.6.6 电子认证服务机构对更新证书的发布

见 4.4.2 电子认证服务机构对证书的发布。

4.6.7 电子认证服务机构对其他实体的通告

关于该证书是否可以正常使用，其它用户可以在 JXCA 的对外的目录服务器上查到。

4.7 密钥更新

4.7.1 证书密钥更新的情形

证书密钥更新条件具体包括：

1、证书的有效期将要到期；

2、密钥对的使用期将要到期；

3、因私钥泄漏而吊销证书后，就需要进行证书更新；

4、其他。

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为证书订户。

4.7.3 证书密钥更新请求的处理

1、JXCA 对证书密钥更新请求的处理通过证书更新请求处理流程完成。

2、JXCA 证书密钥更新请求的处理流程同本 CPS 4.6.3 节描述。

4.7.4 颁发新证书时对订户的通告

见 4.6.4 颁发新证书时对订户的通告。

4.7.5 构成接受密钥更新证书的行为

见 4.4.1 构成接受证书的行为。

4.7.6 电子认证服务机构对密钥更新证书的发布

JXCA在签发更新证书后，就将更新证书发布到目录服务器中，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

证书的变更是指证书用户在名称等有关用户的信息发生变更但密钥不需要改变的情况下，向 RA 提出修改证书内容的情形。

4.8.2 请求证书变更的实体

请求证书变更的实体为证书订户。

4.8.3 证书变更请求的处理

1、JXCA 对证书变更请求的处理通过证书更新请求处理流程完成。

2、JXCA 证书变更请求的处理流程同本 CPS 4.6.3 节描述。

4.8.6 电子认证服务机构对变更证书的发布

见 4.4.2 电子认证服务机构对证书的发布。

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

以下对证书吊销和挂起的情况进行描述

4.9.1 证书吊销的情形

对于下列情况之一，JXCA 将吊销所签发的数字证书：

1、JXCA 发现订户在申请时提供的证明材料不真实；

2、订户没有按照规定缴纳数字证书服务费用；

3、订户未履行证书服务责任书约定的义务；

4、订户要求吊销数字证书；

5、订户主体消亡；

6、订户变更数字证书的用途；

7、私钥失窃、篡改、未经授权的泄露和其它安全威胁；

8、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

请求证书吊销实体为订户、注册机构、JXCA。

4.9.3 吊销请求的流程

- 申请者到 JXCA 授权的发证机构书面填写“证书吊销申请”，并注明吊销的原因。
- JXCA 授权的发证机构按照 3.身份标识与鉴别对用户提交的证书吊销申请进行审核。
- 强制吊销：JXCA 授权的发证机关管理员可以依法对用户证书进行强制挂起，吊销后必须立即通知该证书用户。强制吊销的命令来源于：JXCA 或 JXCA 授权的发证机构。
- JXCA 注销用户证书后，发证机构将通知用户证书被注销。用户证书在 24 小时内进入 CRL 或被直接签发 CRL，向外界公布。

4.9.4 吊销请求宽限期

如果出现密钥泄露或有泄露嫌疑等事件，吊销要求必须在泄密或有泄密嫌疑 8 小时以内提出。其他吊销原因的吊销要求必须在变更的 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

CA 在接到吊销请求后应立即处理且在 24 小时内完成。

4.9.6 依赖方检查证书吊销的要求

依赖方需要访问 JXCA 目录服务器来查询用户的证书状态，以获得用户证书是否可以信赖的信息。

4.9.7 CRL 发布频率

JXCA 将通过证书黑名单列表在 24 小时内公布被吊销的证书，特殊紧急情况下可以立即生效（假使网络传输条件能够保证）。对于测试证书的吊销，不提

供黑名单公布服务。

4.9.8 CRL 发布的最大滞后时间

JXCA 的 CRL 发布最大滞后时间为发布周期之后的 24 小时内。

4.9.9 在线的吊销/状态查询的可用性

使用 JXCA 提供 7×24 小时目录服务，可以进行证书吊销查询和状态查询。

4.9.10 吊销信息的其他发布形式

OCSP 作为可选的吊销通知形式。

4.9.11 证书挂起的情形

以下情况出现时考虑证书挂起：

1、订户怀疑证书或密钥受到攻击。

2、订户违反了 CPS 规定的重要职责。

3、没有按期缴纳证书费。

4.9.14 请求证书挂起的实体

请求证书挂起的实体为订户。

4.9.15 挂起请求的流程

- 申请者到 JXCA 授权的发证机构书面填写“证书废止申请”，并注明挂起的原因。
- JXCA 授权的发证机构按照 3 .身份标识与鉴别对用户提交的证书挂起申请进行审核。
- 强制挂起：JXCA 授权的发证机关管理员可以依法对用户证书进行强制挂起，挂起后必须立即通知该证书用户。强制挂起的命令来源于：JXCA 或 JXCA 授权的发证机构。
- JXCA 挂起用户证书后，发证机构将当面通知或通过发送 E-mail 邮件或

邮寄的方式通知用户证书被挂起；

4.9.16 挂起的期限限制

用户证书被挂起后，用户必须在证书挂起之日起的三十日内申请恢复证书，否则 JXCA 或 JXCA 授权的发证机构有权自行注销证书。对此造成的任何后果，JXCA 不负任何责任。

4.10 证书状态服务

4.10.1 操作特征

订户通过 JXCA 的证书状态查询系统，能够在线查询证书的状态。。

4.10.2 服务可用性

JXCA 的证书状态查询系统能够保持与订户的实时网络连接。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

证书状态的其他可选服务方式为订户利用 JXCA 指定的 CRL 地址，通过目录服务器提供的查询系统，查询并下载 CRL 到本地，进行证书状态的查询。

4.11 订购结束

1、当订户停止使用 JXCA 提供的数字证书时，必须向 JXCA 提出证书注销的申请。申请流程为本 CPS 中 4.9.3 的规定。JXCA 注销证书后，表明订户的订购行为正式结束。

2、当证书有效期结束后，订户未按时续缴服务费时，JXCA 吊销证书后，表明订户的订户行为正式结束。

4.12 密钥生成、备份与恢复

4.12.1 密钥生成、备份与恢复的策略与行为

JXCA 要求订户必须使用本订户的数字证书载体生成签名密钥对。订户可以委托 JXCA 代订户进行生成签名密钥对的有关操作。由于签名私钥遗失所造成的损失由订户自己承担，JXCA 对此不承担责任。

证书订户的加密密钥对由 JXCA 代订户向江西省电子密钥管理中心申请生成，并由江西省电子密钥管理中心进行管理。当证书订户需要恢复加密密钥时，按照江西省电子密钥管理中心的规范、流程，接受订户的申请，为订户恢复相应的加密密钥。

5 认证机构设施、管理和操作控制

本章为 JXCA 系统非技术性安全控制规范，这些规范对于 JXCA 的权威性是十分关键的，安全的控制下将最大限度的减少 CA 遭受攻击的情况发生。

5.1 物理控制

系统的物理安全和环境安全是整个 JXCA 系统安全的基础，它包括基础设施的处理、周边环境的监控、区域访问控制、设备安全及灾难预防等。为把 JXCA 系统的危险减至最低限度，JXCA 选择设施的适当位置，充分考虑水灾、地震、电磁干扰与辐射、犯罪活动以及工业事故等的威胁。

JXCA 系统中的基础设施包括涉及微型计算机和主机、LAN 服务器等资源的房间，对这些设施进行严格的管理，对系统的访问严格控制，并需要经过授权和进行监控，例如有指纹门禁系统、防侵入系统、机械组合锁等装置。

5.1.1 场地位置与建筑

JXCA 主机房位于南昌市区。所有机房的建设和管理严格按照 JXCA 的规定要求，采用高安全性的监控技术，包括视频实时监测、指纹、身份识别卡等监控技术，以确保物理通道的安全。安全区内墙六面全部用钢板焊接，屏蔽较果良好，具有防物理侵入、防电子泄露等高安全性能。

5.1.2 物理访问

机房内部一律禁止参观，只有经过 JXCA 授权的人员才能进入授权的部门和工作地点。在进入 JXCA NOC（JXCA Network Operation Center，简称 NOC）时，必须经过身份识别。NOC 实行全年 24 小时自动监控。监控记录文件包括对 NOC 通道上的所有踪迹的记录。JXCA 的员工经授权后，两人以上才能进入 NOC。对于要进入 NOC 的来访者，要经 JXCA 安全管理小组批准后，指定并授权一位 JXCA 的员工陪同。

5.1.3 电力与空调

JXCA 机房所在的楼内使用两路市电电源至机房配电室，DMZ、RA、CA、KMC 和安监系统、消防控制系统都配有足够容量的 UPS 电源。机房供配电系统经机房配电柜向主机电源、外部设备、辅助设备、空调、照明、门禁、UPS 等提供线制的交流电。电压、频率及额定容量符合终端设备正常运行的技术要求。

5.1.4 水患防治

JXCA 机房的排水系统作为防水设施。

5.1.5 火灾防护

JXCA CA 中心的电器系统符合电子数据处理设备的防火标准、组织政策、职业安全与保健法等。所有设备的电源系统与厂商技术规范保持一致。机房内配备了火情警报及处理装置。按防火管制的要求，尽量减少出入口数量。

JXCA 通过与专业防火部门协调，实施消防灭火等应急响应措施，避免火灾的威胁，充分保障系统安全。

5.1.6 介质存储

JXCA 的存储介质包括硬盘、光盘等，介质存储地点和 JXCA 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

废弃物的处理：纸介质用碎纸机粉碎或焚毁，其他介质以不可恢复原则进行相应的销毁处理。

5.2 程序控制

5.2.1 可信角色

JXCA 系统角色（Role）包括安全管理小组、超级管理员、系统管理员、审计员等。

5.2.2 每个角色的识别与鉴别

所有JXCA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。JXCA将独立完整地记录其所有的操作行为。

5.2.3 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JXCA的可信角色由不同的人担任。

系统管理员和安全审计员岗位不能由同一人担任;RA录入员和RA审核员不能由同一人担任。

5.3 人员控制

5.3.1 资格、经历和无过失要求

JXCA 对 CA 运行人员的背景、资历、经验等情况都进行核实和审查。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。背景:要求政治素质高、业务优秀、有非常强的责任感，原则性强，无犯罪记录和不良记录；资历:要求大专以上学历、熟悉本岗位工作、熟悉系统安全性要求；核实:行政部及用人部门共同负责对 CA 运行人员的背景、资历及经验进行真实性核实。

5.3.2 背景审查程序

JXCA 应检查运行人员的工作经历、接受培训和受到奖惩的情况等背景情况。背景检查程序为：

1、行政部负责对应聘人员的个人资料予以确认。应提供如下资料：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、行政部通过电话、信函、网络、走访、调阅档案等形式对其提供的材料的真实性进行鉴定。
3、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。

4、经考核，行政部和用人部门联合写出背景考察报告，经主管领导批准后准予上岗。

5.3.3 培训要求

JXCA 对运行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、系统备份与恢复 、CA 中心的内部管理政策和规定等。

5.3.4 再培训周期和要求

JXCA 将根据机构系统升级、策略调整等要求，不定期的要求人员进行继续培训。

5.3.5 工作岗位轮换周期和顺序

对于可替换角色，JXCA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 未授权行为的处罚

当JXCA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JXCA系统或进行越权操作，JXCA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

对于不属于 JXCA 机构内部工作人员，但从事 JXCA 业务有关工作的如业务分支机构的业务人员、管理人员等独立签约者，JXCA 的统一要求如下：

1、人员档案的备案管理；

2、具有相关业务的工作经验；

3、必须接受 JXCA 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，这些文档包括：

- 软/硬件、网络设备安全操作手册；
- 加密机、密钥管理安全操作手册；
- RA 系统相关安全操作手册；
- 系统备份与恢复安全操作规范和手册；
- JXCA 电子认证业务规则；
- JXCA 岗位职责说明书；
- JXCA 安全管理制度等。

5.4 审计日志程序

5.4.1 记录事件的类型

JXCA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。

JXCA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

JXCA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

密钥和证书信息档案必须要至少保留 7 年。审计跟踪文档则须保留至少 5 年。

5.4.4 审计日志的保护

JXCA执行严格的管理，确保只有JXCA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，审计日志的制作和访问进行岗位分离

5.4.5 审计日志备份程序

JXCA保证所有的审查记录和审查总结都按照JXCA备份标准和程序进行备份。

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 审计收集系统

由 CA 和 RA 系统以及 CA 和 RA 管理员完成。方式上有系统自动和人工采集方式。

5.4.7 对导致事件实体的通告

如发生事故应立即通知相关的事故责任人和系统管理员。

5.4.8 脆弱性评估

JXCA每年对系统进行脆弱性评估，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

JXCA 数据库的保存期为数据建立时起的 7 年。审计跟踪文档的保存期为审计记录建立时起的 5 年。

5.5.3 归档文件的保护

存档文件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。JXCA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

JXCA 的档案在创建的时候就要进行备份。原件储存在现场，备份文档储存在安全的地方。

5.5.5 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。JXCA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JXCA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。JXCA根密钥由加密机产生，有效期为17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。

5.7 损坏与灾难恢复

5.7.1 事故和损害处理流程

发生故障时，JXCA将按照灾难恢复计划实施恢复。

5.7.2 计算机资源、软件和/或数据的损坏

JXCA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，JXCA将按照灾难恢复计划实施恢复。

5.7.3 实体私钥损害处理程序

当JXCA的私钥被攻破或需要作废时，JXCA根据JXCA灾难恢复计划规定的灾难恢复步骤进行操作。

5.7.4 灾难后的业务连续性能力

灾难发生后 JXCA 立即用备用系统上线对用户提供服务，保持业务持续性。

5.8 电子认证服务机构或注册机构的终止

5.8.1 CA 终止原因

JXCA 终止事件的原因可以分为密钥受损原因和非密钥受损原因。密钥受损原因可能包括 JXCA 根密钥丢失，非密钥受损原因可能与商业因素有关。

5.8.2 终止通知

当 JXCA 打算终止经营时，会在终止经营前三个月给 JXCA 授权的发证机构和证书持有者书面通知，并在终止服务六十日前向国务院信息产业主管部门报告，按照相关法律规定的步骤进行操作。

5.8.3 终止归档

JXCA 会按照相关法律的规定来安排好档案和证书的存档工作。

5.8.4 终止措施

在 CA 中止期间，采用以下措施终止业务：

- 起草 CA 终止声明；
- 通知与 CA 停止相关的实体；
- 关闭从目录服务器；
- 证书注销；
- 处理存档文件记录；
- 停止认证中心的服务；

- 存档主目录服务器；
- 关闭主目录服务器；
- 管理 JXCA 系统管理员和 JXCA 安全官员；
- 处理加密密钥；
- 处理和存储敏感文档；
- 清除 CA 主机硬件。

5.8.5 RA 的终止根据

根据 JXCA 与 RA 签订的协议终止 RA 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

由于密钥对是安全机制的关键，所以在认证业务声明中制定了相应的规定，确保密钥对的产生、传送、安装等具备保密性、完整性和不可否认性。

6.1.1 密钥对的生成

- 加密密钥对

加密密钥对是由中华人民共和国国家密码管理委员会（以下简称国密委）许可的、JXCA 数字证书签发系统支持的加密机设备生成的，由江西省国家密码管理局所属的 KMC 控制管理。

- 签名密钥对

签名密钥对由客户端产生，证书申请者可使用江西省国家密码管理局认可的、JXCA 数字证书签发系统支持的介质生成签名密钥对。签名密钥存储在介质中不可导出，保证 JXCA 无法复制签名密钥对。

JXCA 支持多种介质，如智能密码钥匙。JXCA 可根据证书申请者要求或自身选择签名密钥对生成介质。

JXCA 在技术、流程和管理上保证密钥对产生的安全性。

6.1.2 私钥传送给订户

证书用户的加密私有密钥是在 KMC 产生的，该私有密钥只保存在 KMC。在加密私有密钥从 KMC 到用户的传递过程中采用国密委许可的密钥算法加密。JXCA 无法获得，保证了证书用户的密钥安全。

6.1.3 公钥传送给证书签发机构

JXCA 从 KMC 取得用户公钥后为其签发证书，在此过程中也采用国密委许可的密钥算法加密，保证传输中数据的安全。

6.1.4 电子认证服务机构公钥传送给依赖方

JXCA 的根公钥包含在 JXCA 自签的根证书中。证书用户可以从 JXCA 的网站上下载 JXCA 根证书。

6.1.5 密钥的长度

JXCA 所使用的密钥对长度支持 1024 位。

6.1.6 公钥参数的生成和质量检查

JXCA 系统使用由国密委许可的密钥生成算法、JXCA 数字证书签发系统支持的硬件生成随机数作为公钥参数。

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

JXCA 所用的密码设备都是经国密局认可的产品，其安全性达到以下要求：

1、接口安全：不执行规定命令以外的任何命令和操作；

2、协议安全：所有命令的任意组合，不能得到私钥的明文；

3、密钥安全：密钥的生成和使用必须在硬件密码设备中完成；

4、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 私钥多人控制（m 选 n）

为保证系统运营安全，对CA私钥的相关敏感操作都采取五选三方式，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，才能对私钥进行相应的操作。

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。

6.2.4 私钥备份

订户的签名密钥JXCA和KMC都不备份。加密私钥由KMC备份，确保加密私钥的安全。

6.2.5 私钥归档

KMC 提供过期的托管私有密钥的存档服务。

6.2.6 私钥导入、导出密码模块

在 JXCA 证书服务体系中，使用 JXCA 的软件可以把私有密钥导入密码模块中。

私有密钥无法从硬件及软件密码模块中导出。必须通过密码验证之后，才可能使用存储在密码模块中的私有密钥进行加解密操作。

6.2.7 私钥在密码模块的存储

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密钥登录，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密钥登录，

启动密钥管理程序，进行解除私钥激活状态的操作，需要三名管理员同时在场。

6.2.10 销毁私钥的方法

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

6.2.11 密码模块的评估

JXCA使用成都卫士通的SJY15-C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：

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16Mbps；模长1024的数字签名速度111次/秒。

6.3 密钥对管理的其它方面

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JXCA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

JXCA 根证书有效期为 10 年，用户证书由于考虑到安全性，目前提供的证书有效期一般为一年，但系统支持在根证书有效期内的任意期限，最短可定制到

一天。

6.4 激活数据

6.4.1 激活数据的产生和安装

JXCA 产生的激活数据，包括用于通讯的加密密钥、USB Key 的 PIN 码等，都是在安全可靠的环境下，由硬件设备产生（建议 PIN 码都为至少 6 位以上）。

这些激活数据，都通过安全可靠的方式，例如离线当面递交、邮政专递等方式交给订户。

6.4.2 激活数据的保护

订户的激活数据必须进行妥善保管，或者记住以后进行销毁，不可被他人所获悉。如果有书面保留的需求时，必须进行安全可靠的保存。同时，为了配合业务系统的安全需要，应该经常对激活数据进行修改。

6.4.3 激活数据的其他方面

私钥保护密码在使用中可以修改以提高其安全性。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

JXCA 数字证书签发系统的数据文件和设备由 JXCA 系统管理员维护，未经 JXCA 管理员授权，其它人员不能操作和控制 JXCA 系统。JXCA 系统部署在多级不同厂家的防火墙之内，确保系统网络安全。

JXCA 系统密码有最小密码长度要求，而且必须符合复杂度要求，JXCA 系统管理员定期更改系统密码。

6.5.2 计算机安全评估

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

JXCA 的认证系统，通过了国家密码管理局的安全性审查。

6.6 生命周期技术控制

6.6.1 系统开发控制

JXCA 应用软件开发和控制遵循以下原则：

- 第三方的验证和审核；
- 安全风险分析和可靠性设计。

同时，JXCA 的软件开发操作规范，参考 ISO15408 的标准，执行相关的规划和开发控制。

6.6.2 安全管理控制

JXCA 的配置以及任何修改和升级都会记录在案并进行控制，并且 JXCA 采取一种灵活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。

6.6.3 生命期的安全控制

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。JXCA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。

7 证书、证书吊销列表和在线证书状态协议

7.1 证书

7.1.1 版本号

JXCA 证书有广泛的通用性。证书格式符合 X.509 V3 标准，可以提供支持证书扩展的能力。

7.1.2 证书扩展项

JXCA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。

JXCA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。

7.1.3 算法对象标识符

JXCA 签发的证书中，密码算法的标识符为 sha1RSA。

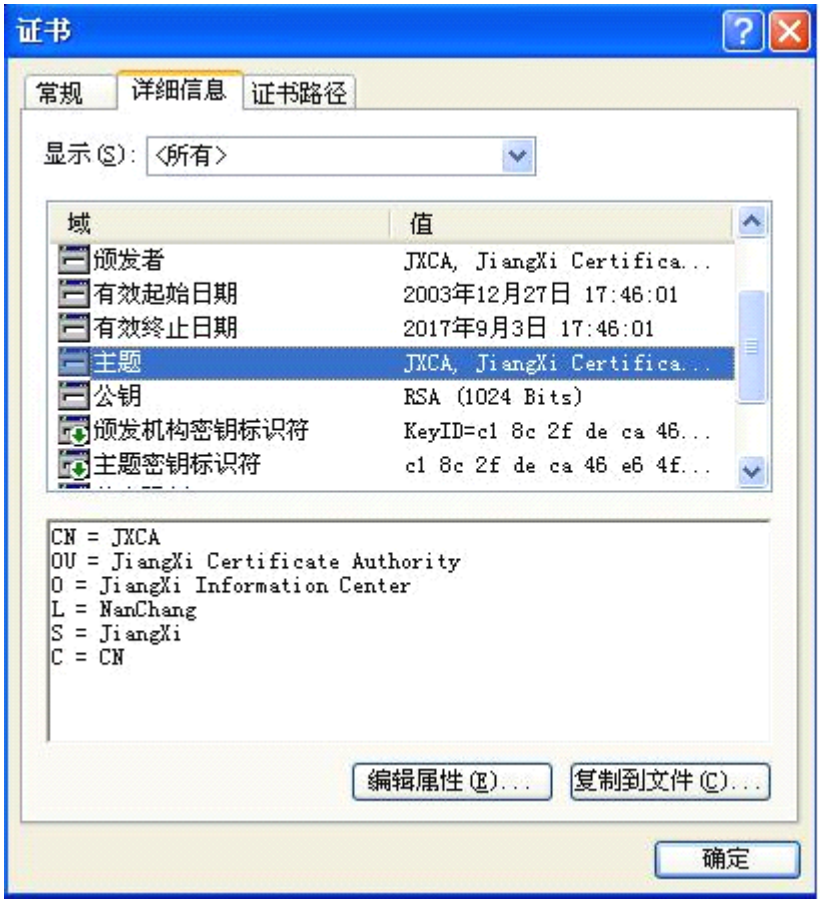
7.1.4 名称形式

采用 X.500 甄别名格式，详见 3.1 节。

- 策略标识

  暂无。

- 示图



7.1.5 名称限制

JXCA 签发的证书，其识别名称不允许为匿名或者伪名，必须是有确定含义的识别名称。

7.2 证书吊销列表

JXCA 定期签发 CRL（证书吊销列表），其所签发的 CRL。采用 X.509V2 格式。

7.2.1 版本号

X.509：V2。

7.2.2 CRL 和 CRL 条目扩展项

- 颁发者

  CN = JXCA

  C = CN

- CRL 发布

  JXCA 每隔 24 小时自动发布最新的 CRL。

- 签名算法

  JXCA 采用 sha1RSA 签名算法。

7.2.3 示图

7.3 在线证书状态协议

JXCA 为证书用户提供 OCSP（在线证书状态查询服务），OCSP 为 CRL 的有效补充，方便证书用户及时查询证书状态信息。

7.3.1 版本号

- OCSP：V1。

7.3.2 OCSP 扩展项

- 暂无。

8 认证机构审计和其它评估

8.1 评估的频率或情形

审计是为了检查、确认 JXCA 是否按照《电子认证业务规则》及其业务规范、管理制度和安全策略开展业务，发现存在的可能风险。审计分内部审计和外部审计。

内部审计是由 JXCA 自己组织内部人员进行的审计，审计的结果可供 JXCA 改进、完善业务，内部审计结果不需要公开。

外部审计由 JXCA 委托第三方审计机构来承担，审计的依据包括 JXCA 所有与业务有关的安全策略、《电子认证业务规则》、业务规范、管理制度，以及国家或行业的相关标准。

8.2 评估者的资质

内部审计人员的选择一般包括：

- JXCA 的安全负责人及安全管理人员；
- JXCA 业务负责人；
- 认证系统及信息系统负责人；
- 人事负责人；
- 其他需要的人员。

外部审计的审计人员的资质由第三方确定。。

8.3 评估者与被评估者的关系

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

JXCA 的审计工作包括以下内容：

1、安全策略是否得到充分的实施；

2、运营工作流程和制度是否得到严格遵守；

3、是否严格按 CPS、业务规范和安全要求开展认证业务；

4、各种日志、记录是否完整，是否存在问题；

5、是否存在其他可能存在的安全风险。

8.5 对问题与不足采取的措施

对审计中发现的问题，JXCA 将根据审计报告的内容准备一份解决方案，明确对此采取的行动。JXCA 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

除非法律明确要求，JXCA 一般不公开评估结果。

对 JXCA 关联方，JXCA 将依据签署的协议来公布评估结果。

9 法律责任和其他业务条款

9.1 费用

9.1.1 证书签发和更新费用

数字证书的收费标准按照国家和江西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，JXCA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

JXCA 保留对占用大量 JXCA 资源的用户证书查询操作进行收费的权利。

9.1.3 证书吊销或状态信息的查询费用

JXCA 保留对占用大量 JXCA 资源的用户证书吊销和状态信息查询操作进行收费的权利。

9.1.4 其它服务费用

JXCA 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，JXCA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，JXCA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，JXCA将不退还剩余时间的服务费用。

9.2 财务责任

9.2.1 赔偿责任范围

JXCA 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 JXCA 原因，致使订户无法正常验证证书状态，导致订户利益受损。

3、JXCA 在证书有效期限内承担损失或损害赔偿。

9.2.2 对最终实体的赔偿担保

JXCA 对所有当事实体（包括但不限于订户、申请人或信赖方）的合计责任不超过证书的适用的责任封顶。对于一份证书产生的所有数字签名和交易处理，JXCA 对于任何人有关该特定证书的合计责任应该限制在一个不超出赔偿责任上限的范围内，这种赔偿上限可以由 JXCA 根据情况重新制定，JXCA 会将重新制定后的情况立刻通知相关当事人。

JXCA 所颁发数字证书的赔偿责任上限如下。

个人证书：500 元人民币。

机构证书：2000 元人民币。

服务器证书：8000 元人民币。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的责任均有封顶而不考虑数字签名和交易处理等有关的其他索赔的数量。当超过责任封顶时，可用的责任封顶将首先分配给最早得到索赔解决的一方。JXCA 没有责任为每个证书支付高出责任封顶的赔偿，而不管责任封顶的总量在索赔提出者之间如何分配。

9.2.3 责任免除

有下列情况之一的，应当免除 JXCA 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 JXCA 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，JXCA 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、JXCA 不承担任何其他未经授权的人或组织以 JXCA 名义编撰、发表或散布的不可信赖的信息所引起的法律责任。

3、JXCA 不承担在法律许可的范围内，根据受害者或法律的要求如实提供网上业务中“不可抵赖”的数字签名依据所引起的法律责任。

4、JXCA 不对任何一方在信赖证书或使用证书过程中引起的直接或间接的损失承担责任。

5、JXCA 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。JXCA 和证书持有人间的关系以及 JXCA 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 JXCA 承担信托责任。

6、由于客观意外或其他不可抗力事件原因而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。关于不可抗力的描述参见 9.16.4。

7、因 JXCA 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、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。

8、JXCA 已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

9.3 业务信息保密

9.3.1 保密信息范围

保密信息有但不限于以下方面：

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机密数据和信息的；

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 JXCA 来说有但不限于以下方面：

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应是保密的。

3、年度审计结果也同样视为保密。

4、除非有法律要求，由 JXCA 掌握的，除作为证书、CRL、认证策略被发布之外的个人和公司的信息需要保密。

5、JXCA 不保存任何证书应用系统的交易信息。

除非法律明文规定，JXCA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。JXCA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JXCA目录服务等方式向外公布。

JXCA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JXCA在任何法律、法规或规章的要求下，或在法院的要求下必须提供本《电子认证业务规则》中具有保密性质的信息时，JXCA应按照要求，向执法部门公布相关的保密信息，JXCA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，JXCA保证不会截取任何证书申请人的资料。

JXCA应保护证书申请人所提供的，证明其身份的资料。JXCA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 不被视作隐私的信息

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JXCA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与同意

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JXCA在任何法律、法规或规章的要求下，或在法院的要求下必须提供证书申请人的特定资料或隐私信息时，JXCA按照法律、法规或规章的要求或法院的要求，向执法部门公布相关信息，JXCA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 其它信息披露情形

其他信息的披露遵循国家的相关规定处理。

9.5 知识产权

JXCA 享有并保留对证书以及 JXCA 提供的全部软件的独一无二的一切知识产权，包括保证证书和软件的完整权、名称权和利益分享权等。因此，JXCA 有权决定关联机构采用什么软件系统，选择采取的形式、方法、时间、过程和模型，以便保证系统的兼容和互通。

按本认证业务规则的规定，所有与 JXCA 发行的证书和 JXCA 提供的软件相关的一切版权、商标和其他知识产权均属于 JXCA 的产权，这些知识产权包括所有相关的文件和使用手册。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

JXCA在提供电子认证服务活动过程中的承诺如下：

1、JXCA遵守《中华人民共和国电子签名法》及相关法律的规定，接受信息产业主管部门的领导，对签发的数字证书承担相应的法律责任。

2、JXCA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JXCA证书库发出了JXCA的私钥被破坏或被盗的通知，JXCA保证其私钥是安全的。

4、JXCA签发给订户的证书符合JXCA的CPS的所有实质性要求。

5、JXCA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、JXCA将及时吊销证书。

7、JXCA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，JXCA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

JXCA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JXCA的CPS的所有实质性要求。

2、在JXCA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CPS的规定，及时向JXCA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JXCA签发的证书，就被视为向JXCA、注册机构及信赖证书的有关当事人作出以下承诺：

1、订户需熟悉本《电子认证业务规则》的条款和与其证书相关的证书政策，还需遵守证书持有人证书使用方面的有关限制。

2、订户在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JXCA或注册机构检查和核实。

3、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。

4、私钥为订户本身访问和使用，订户对使用私钥的行为负责。

5、一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄密以及其他情况，订户应立刻通知JXCA和注册机构，申请采取吊销等处理措施。

6、订户已知其证书被冒用、破解或被他人非法使用时，应及时通知JXCA吊销其证书。

9.6.4 依赖方的陈述与担保

证书依赖方向 JXCA、注册机构、订户等认证实体作出以下承诺：

1、信赖 JXCA 签发的数字证书。

2、遵守本 CPS 的所有规定。

3、采取合理步骤，查证订户数字证书及数字签名的有效性。

9.6.5 其它参与者的陈述与担保

JXCA 从事电子认证活动的其他参与者作出如下承诺：

遵守本 CPS 的所有规定。

9.7 担保免责

除非在本 CPS 9.6.1 中的明确承诺外，JXCA 不承担其他任何形式的保证和义务。同时，JXCA 将：

1、不保证证书订户、信赖方、其他参与者的陈述内容。

2、订户违反本 CPS 9.6.3 之承诺时，或证书依赖方违反本 CPS 9.6.4 之承诺时，得以免除 JXCA 之责任。

3、不对电子认证活动中使用的任何软件作出保证。。

9.8 有限责任

JXCA 在与用户和依赖方签订的协议中，对于因用户或依赖方的原因造成的损害不具有赔偿义务。

9.9 赔偿

JXCA按照本《电子认证业务规则》9.2条款承担赔偿责任。

证书订户和依赖方在使用或信赖证书时，若有任何行为或疏漏而导致JXCA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JXCA提供真实、完整和准确的信息，而导致JXCA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JXCA，并终止使用该证书，而导致JXCA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JXCA对证书使用的规定，造成了JXCA或有关各方的利益受到损失。

9.10 有效期限与终止

9.10.1 有效期限

本 CPS 及其更新版本自公布之日起的 15 天之后正式生效。

9.10.2 终止

当新版本的《电子认证业务规则》正式发布生效时，旧版本的《电子认证业务规则》自动终止。

在JXCA终止电子认证服务时，本CPS也同时终止。

9.10.3 效力的终止与保留

在协议终止的情况下，有些条款依然是保留的，例如知识产权，需要继续履行。各方需要归还或保证销毁从其它方获得的机密信息。

9.11 对参与者的个别通告与沟通

JXCA 体系中各参与方之间都建立或具有个别沟通的渠道。

9.12 修订

9.12.1 修订程序

修正的流程为：

1、发现 CPS 中所列条款不能适应运营的实际需求，或者与现行法律相抵触；

2、将现存问题反馈 CPS 编写组；

3、经过 CPS 编写组讨论后，提出具体的修改意见；

4、修改意见提交运营安全管理小组；

5、运营安全管理小组审查修改意见，如果不通过则提出修改意见反馈 CPS

编写组；

6、CPS 修改意见经运营安全管理小组审查通过，由 CPS 编写组发布更新。

9.12.2 通知机制和期限

修订后的新版 CPS，JXCA 将通过网站方式予以公布。新版 CPS 将在自公布之日起的 15 天后生效。

9.12.3 必须修改业务规则的情形

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

9.13 争议处理

JXCA、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、根据本 CPS 中的规定，明确责任方；

2、由 JXCA 相关部门负责与申请人协调；

3、若协调失败，再由有关法律部门进行裁决。

4、任何与 JXCA 或授权机构就本 CPS 所涉及的任何争议提起诉讼的，受 JXCA 工商注册所在地人民法院管辖。。

9.14 管辖法律

JXCA CPS 和协议中条款的制定遵守《中华人民共和国合同法》和《中华人民共和国电子签名法》。

9.15 与适用法律的符合性

JXCA 的各项策略遵守和适应中华人民共和国各项法律法规和国家信息安全主管部门要求。

9.16 一般条款

9.16.1 完整协议

现行条款替代所有以前的和同时期的条款。

9.16.2 转让

JXCA 声明，根据本 CPS 中详述的认证实体各方的权利和义务，各方当事人可按照法律的相关规定进行权利和义务的转让。此转让行为发生时不影响到转让方对另一方的任何债务及责任的更新。

9.16.3 分割性

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

9.16.4 强制执行

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

9.16.5 不可抗力

由于不可预见的原因和不可控的原因，视为不可抗力，会导致合同或协议的终止。例如战争、恐怖行动、罢工、自然灾害、供货商或代理商倒闭、互联网或其它基础设施无法使用等。在数字证书认证活动中，JXCA 由于不可抗力因素而暂停或终止全部或部分证书服务的，可根据不可抗力的影响而部分或者全部免除违约责任。其他认证各方（如订户）不得提出异议或者申请任何补偿。

9.17 其它条款

JXCA 对本 CPS 具有最终解释权。