江西省数字证书有限公司
电子认证业务规则

2.1 版

发布日期：　　2019 年 3 月 29 日

生效日期：　　2019 年 3 月 29 日

江西省数字证书有限公司

版本控制表

版本	状态	修订说明	审核/批准人	生效时间
2.0	版 本发布	新版本发布	江西CA安全策略委员会	2007年7月10日
2.1	修订	1、增加机构个人证书 2、更新身份鉴别 3、简称“JXCA”替换为“江西CA” 4、删除“9.支持服务管理”内容 5、原“10.法律责任和其他业务条款”更换为“9.法律责任和其他业务条款”	江西CA安全策略委员会	2019年3月29日

目录

1 概括性描述

1.1 概述

江西省数字证书有限公司电子认证业务规则（以下简称“江西 CA CPS”）由江西省数字证书有限公司按照工业和信息化部《电子认证服务管理办法》的要求，依据《电子认证业务规则规范（试行）》制定。

本 CPS 详细阐述了江西 CA 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、吊销、更新、变更、挂失等操作流程；信息公开的要求等内容以及在实际工作和运行中应遵循的各项规范。对于江西 CA 所提供的认证服务过程的责任范围，本业务规则也给予了明确的规定。

1.2 文档名称与标识

本文档名称为《江西省数字证书有限公司电子认证业务规则》，简称为江西 CA CPS，是江西 CA 对所提供的认证及相关服务的全面描述。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

江西 CA 是根据《中华人民共和国电子签名法》及《电子认证服务管理办法》规定,依法设立的电子认证服务机构，是电子政务、电子商务活动中可信赖的第三方机构。江西 CA 为电子政务和电子商务的各参与方签发标识其身份的数字证书，并承担对数字证书进行签发、更新、吊销、密钥管理、证书查询等一系列管理工作，保证各参与方主体身份的真实性、信息的保密性和完整性以及行为的不可抵赖性。

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（简称：RA 系统）和证书受理点，负责受理证书申请。

1.3.3 订户

在电子签名应用中，订户即是电子签名人、证书持有人，是江西 CA 颁发证书的所有最终用户，可以是个人、机构或基础设施的组成部件如路由器、防火墙、服务器或用于安全通信的其他设备。

1.3.4 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。依赖方可以是或不是一个订户。在 CA 证书服务体系中，是信任 CA 机构证书，可以对使用 CA 机构证书机制进行的数字签名进行验证，使用 CA 机构证书的公钥的实体。

1.3.5 其他参与者

其他参与者是指为江西 CA 的电子认证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

江西 CA 签发的数字证书适用于电子商务、电子政务、及其他社会信息化的应用中，以实现身份认证、电子签名、关键数据加密等目的，同时也保障互联网上信息传递双方身份的合法性和真实性以及信息的完整性和保密性。

目前江西 CA 可以签发的证书种类有以下五类：

1）个人数字证书

2）机构个人证书

3）机构数字证书

4）设备证书

5）代码签名证书

1.4.2 限制的证书应用

本 CA 机构发放的数字证书禁止在违反国家法律、法规或破坏国家安全的情况下使用，由此造成的法律后果由订户负责。

1.5 策略管理

1.5.1 策略文档管理机构

江西 CA CPS 的管理机构是江西 CA 安全策略委员会。由江西 CA 安全策略委员会授权 CPS 编写小组负责江西 CA CPS 的制订、更新、发布等事宜。

1.5.2 联系人

江西 CA CPS 在江西 CA 网站发布，对具体个人不另行通知。

网站地址：http://www.jxca.org.cn

电子邮箱地址：jxca@jxca.org.cn

联系地址：江西省南昌市省府大院西二路 3 号

电话号码：0791-88858083

传真号码：0791-86222510

1.5.3 决定CPS符合策略的机构

作为电子认证业务的主管部门，工业和信息化部发布了《电子认证业务规则规范（试行）》，江西 CA 根据规范的要求，制定本电子认证业务规则，并提交工业和信息化部备案。

江西CA安全策略委员会是审定批准CPS、决定CPS符合策略的机构，拥有对江西CA CPS的决策权和审批权。

1.5.4 CPS 批准程序

本CPS由江西CA安全策略管理委员会组织CPS编写小组编写。CPS编写小组完成后，提交江西CA安全策略管理委员会审核。经江西CA安全策略管理委员会批准后，正式在江西 CA 网站上对外公布。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，江西CA在公布CPS后向工业和信息部备案。

1.6 定义和缩写

1.6.1 术语定义一览表

电子认证业务规则	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。
电子认证服务机构	受用户信任，负责创建和分配公钥证书的权威机构。
注册机构	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，在某些环境下主动吊销或挂起证书，处理订户吊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。
证书策略	是一个有关证书业务策略的主要说明。
电子签名认证证书	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。

证书吊销列表	一个经电子认证服务机构数字签名的列表，标记已经被吊销的证书列表，也称黑名单服务。
私钥（电子签名制作数据）	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。
公钥（电子签名验证数据）	是指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。

1.6.2 缩略语及其含义一览表

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
CP	CertifiCAte Policy	证书策略
PKI	Public Key Infrastructure	公共密钥基础设施
PIN	Personal IndentifiCAtion Number	证书个人识别码
PKCS	Public KEY Cryptography Standards	公共密钥密码标准

2 信息发布与信息管理

2.1 认证信息的发布

江西 CA 通过网站公布以下信息：江西 CA CPS 修订以及其他由江西 CA 不定期发布的信息。

江西 CA 网址：http://www.jxca.org.cn

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江西 CA 机构本身。订户通过 LDAP、CRL 及 OCSP 服务器获取相关信息，江西 CA 承诺发布的信息及时可靠。

2.2 发布的时间或频率

1、CPS 一经网站发布，即时生效。

2、证书的发布：在证书签发时，江西 CA 通过 LDAP 服务器自动将该证书公布。

3、江西 CA 的 CRL 至少每 24 小时发布一次。

江西 CA 通过网站方式公布本机构制定的 CPS。对于因认证业务需要修改的 CPS 不定期变更，江西 CA 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。江西 CA 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 和证书信息，江西 CA 允许任何公众查询和访问。证书和 CRL 通过 LDAP 方式予以发布，同时提供 OCSP 在线验证方式。江西 CA 采取网络安全防护、授权管理员和安全审计等安全管理手段，确保只有经过授权的人员才能进行信息库的增加、删除、修改、发布等操作。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

江西 CA 颁发的数字证书，含有颁发机构和证书订户主体甄别名，对证书申请者的身份和其它属性进行鉴别，并以不同的标识记录其信息。证书持有者的标识命名，以甄别名（Distinguished Name）形式包含在证书主体内，是证书持有者的唯一识别名。江西 CA 的证书符合 X.509 标准，分配给证书持有者实体的甄别名，采用 X.501 标准命名方式。

3.1.2 对名称意义化的要求

DN(甄别名)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、机构订户的统一社会信用代码等。

3.1.3 订户的匿名或伪名

本 CPS 中明确声明，江西 CA 不接受或者允许任何匿名或者伪名，仅接受有明确意义的名称作为唯一标识符。除非在某些具有特殊要求的电子政务应用中，根据信息保密的要求，江西 CA 根据政务机构出具的相关函件并按照一定的规则为用户指定特殊的名称，并且能够把该类特殊的名称与一个确定的实体（个人、单位或者设备）唯一的联系起来。

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、E、L、S、C 几部分组成。例如：CN 用来表示用户名，OU 表示证件号码，O 表示单位名称，E 表示电子邮箱，L 表示地址，S 表示省，C 表示国家。

3.1.5 名称的唯一性

江西 CA 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

江西 CA 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。本 CA 机构在为通用证书订户签发证书前，系统将自动使用订户的公钥验证其私钥签名的有效性和申请数据的完整性，以此来判断订户拥有私钥。或者江西 CA 要求的其它证明方式，包括提交的初始化信息（被分配的密钥存储介质和对应的 PIN 码）等。

3.2.2 组织机构身份的鉴别

对于组织身份的鉴别，江西 CA 需要验证组织的合法证件。证书申请人需持营业执照或信用代码证书等证件，以及经办人身份证件，向江西 CA 提出申请。

组织身份的鉴别规范简要说明了如何进行组织身份鉴别。江西 CA 保留根据最新国家政策法规的要求更新组织身份鉴别规范的权利。

经办人携带本人身份证的原件和复印件，到 CA 机构或授权的注册机构提交书面数字证书申请表(一式三联)及下述组织证明文件等申请资料，并缴纳证书服务费用。

1、含有统一社会信用代码的证件原件及复印件，如果组织没有含有统一社会信用代码的证件，则可选择提供其他有效证件的原件及复印件，部分有效证件如下：

（1）组织机构代码证

（2）事业单位法人证书

（3）社会团体登记证

（4）医疗机构许可证

（5）政府批文

（6）其他有效证件

2、经办人有效身份证件的原件和复印件；

注：以上1、2证明文件的复印件须加盖申请单位公章。

注册机构对申请资料的原件和复印件真实性进行审核，审核通过后进行批准申请或拒绝申请的操作。

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

3.2.3 个人身份的鉴别

个人身份的鉴别可以使用以下有效的身份证件：身份证、护照、港澳居民来往内地通行证等。

个人身份的鉴别规范简要说明了如何进行个人身份鉴别。江西CA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。

个人需持个人有效身份证件，到注册机构提交书面数字证书申请表(一式三联)和有效身份证件的复印件等申请资料，并缴纳证书服务费用。

注册机构对申请资料的原件和复印件真实性进行审核，审核通过后进行批准申请或拒绝申请的操作。

批准申请后，注册机构将保留复印件，与证书申请表一并存档保存。

3.2.4 机构个人用户身份的鉴别

对于以机构名义申请的个人证书，向该类用户批量签发证书前，必须对该证书申请机构的个人身份进行查验和鉴别。机构类个人身份的鉴别可以使用以下身份证明文件：经办人身份证、机构出具的说明文件并加盖公章，说明文件中至少

包含证书申请人的身份信息。

江西 CA 保留根据最新国家政策法规的要求更新机构个人身份鉴别规范的权利。

经办人需持个人有效身份证件，到注册机构提交上述有效身份证明文件等申请资料，并缴纳证书服务费用。

注册机构对申请资料的真实性进行审核，审核通过后进行批准申请或拒绝申请的操作。

批准申请后，注册机构将保留经办人身份证复印件和机构出具的说明文件并存档保存。

3.2.4 没有验证的订户信息

订户提交鉴证文件（不包括证书申请表）以外的信息为没有验证的订户信息。

3.2.5 授权确认

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

3.2.6 互操作准则

对于其他的电子认证服务机构，可以与江西 CA 进行互操作，但是该电子认证服务机构的 CPS 必须符合江西 CA 的证书策略要求，并且与江西 CA 签署相应的协议。

江西 CA 将依据协议的内容，接受非江西 CA 的发证机构鉴别过的信息，并为之签发相应的证书。

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

在订户证书到期前，订户需要获得新的证书以保持证书使用的连续性。江西CA一般要求订户产生一个新的密钥对代替过期的密钥对，称作“密钥更新”。

对于一般正常情况下的更新密钥申请，订户须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、PING码等，对申请的鉴别基于以下几个方面：

1、申请对应的原证书存在并且由本认证机构签发；

2、基于原注册信息进行身份鉴别。

3.3.2 吊销后密钥更新的标识与鉴别

发证机构不提供证书被吊销后的密钥更新。订户必须重新进行身份鉴别和注册，向江西CA申请重新签发证书。

3.4 吊销请求的标识与鉴别

如果是因为订户没有履行本CPS所规定的义务，由江西CA机构或授权的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。

如果订户主动要求吊销证书，则按照本CPS第3.2节描述进行身份鉴别。

4 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

证书申请者，包含个人、企业单位、事业单位、政府机构、社会团体、人民

团体等各类组织机构。任何合法的组织、个人和有明确身份归属的其他网络主体均可申请数字证书，以保证网上交易和网上行政作业的安全和可靠。

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，通过现场面对面或其他方式提交证书申请，包括相关的身份证明材料。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。

订户：订户需要提供 3.2 所述的有效身份证明材料，并确保材料真实准确。配合注册机构完成对身份信息的采集、记录和审核。

CA机构：CA机构参照3.2的要求对订户的身份信息进行采集、记录，审核。通过鉴证后，CA机构向订户签发证书。如果用户身份信息的鉴别由授权的注册机构完成，CA机构应对授权的注册机构进行监督管理和审计。

根据《中华人民共和国电子签名法》的规定，证书申请者未向 CA 机构提供真实、完整和准确的信息，或者有其他过错，给 CA 机构或电子签名依赖方造成损失的，应承担相应的法律责任和经济赔偿。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

江西 CA 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.身份标识与鉴别。

4.2.2 证书申请批准和拒绝

江西 CA 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，江西CA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，江西 CA 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

江西 CA 授权的注册机构将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江西CA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

江西 CA 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

发送密码的方式根据江西CA证书的申请对象不同，可以分以下几种方式：

1、通过面对面的方式，通知申请者(如申请者到受理点领取等方式)；

2、通过电子邮件(e-mail)方式通知；

3、电话或短信通知；

4、江西CA认为其他安全可行的方式。

4.4 证书接受

4.4.1 构成接受证书的行为

在申请者完成申请程序，江西 CA 和其授权的证书注册机构将证书本身、或者证书获得的方式、或者与证书相关的密码递送给申请者，就意味着申请者已经接受了证书。订户接受数字证书后，应妥善保存与其证书对应的私钥。

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；

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、订户反对证书或者证书内容的操作失败。

4.4.2 电子认证服务机构对证书的发布

订户接受证书后，江西 CA 在其规定的时间内将该订户证书发布到江西 CA 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江西 CA 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 CA 机构所签发的证书后，均视为已经同意遵守与 CA 机构、依赖方有关的权利和义务的条款。

证书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：

1、用 CA 机构的证书验证证书中的签名，确认该证书是 CA 机构签发的，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、检验证书有效性，需要检查该证书没有被吊销。

如果证书中的某些字段明确了证书的使用范围和用途，那么该证书将在也只被允许在这一范围内进行使用。依赖方必须对此做出合理的判断，任何对超出证书所标明的适用范围的行为的信赖，都将由依赖人独立承担责任，江西 CA 对此不承担任何责任和义务。

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、PING 码等，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

证书更新的原因：

1、证书在有效期内延期；

2、证书已到期延期。

证书更新指江西 CA 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证书。

申请证书更新无需填写注册信息，系统会自动获取所需的信息。

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

证书更新时无需提交证书注册信息，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、PIN 码等。

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，通知申请者(如申请者到受理点领取等方式)；

2、通过电子邮件(e-mail)方式通知；

3、电话或短信通知；

4、江西 CA 认为其他安全可行的方式。

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，其它用户可以在江西 CA 的对外的目录服务器上查询。

4.7 密钥更新

4.7.1 证书密钥更新的情形

证书密钥更新是指订户生成新密钥并申请为新公钥签发新证书，CA 机构提供证书更新时，密钥必须同时更新。

证书密钥更新的具体情形如下：

1、当订户证书即将到期或已经到期时；

2、当订户证书密钥遭到损坏时；

3、当订户证实或怀疑其证书密钥不安全时；

4、其它可能导致密钥更新的情形。

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

见本 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

江西 CA 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，向注册机构提出修改证书内容的情形。只有证书在有效期内，才可能发生证书变更。在证书内包含的订户信息发生变化时，订户必须申请进行证书变更，以确保不影响依赖方对证书的信任。

如果证书内包含信息的变更可能影响订户权利义务的改变，则订户不能申请证书变更，只能吊销该证书，再重新申请新的证书。

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

证书变更按照初次申请证书的注册过程进行处理。

4.8.4 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。

4.8.5 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。

4.8.6 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

订户、电子认证服务机构、法院或者政府权力部门等可以要求将证书吊销。

证书吊销后，证书持有者可以重新向江西 CA 或证书业务受理点申请数字证书，与第一次申请时的程序手续相同。

目前，江西 CA 不提供证书挂起服务。一旦提供挂起服务，江西 CA 将会通过网站等进行公布。

4.9.1 证书吊销的情形

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。

发生下列情形之一的，CA 机构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

请求证书吊销实体为订户、注册机构、江西 CA、法院或政府主管部门及其他公权力部门。

4.9.3 吊销请求的流程

证书吊销请求的处理采用与原始证书签发相同的过程。

1、数字证书吊销的申请人到CA机构或授权的注册机构书填写“证书申请表”，勾选“吊销”并注明吊销原因；

2、CA 机构或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、CA 机构吊销订户证书后，在 24 小时内通过 CRL 向外界公布；

4、强制吊销是指当 CA 机构或 CA 授权的注册机构确认用户违反本《电子认证业务规则》的情况发生时，对订户证书进行强制吊销，吊销后将在 24 小时内通过 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

江西 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

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。

4.9.7 CRL 发布频率

CA 机构可采用实时或定期的方式发布 CRL。颁发 CRL 的频率根据证书策略确定，一般为 24 小时定期发布。

4.9.8 CRL 发布的最大滞后时间

江西 CA 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 在线状态查询的可用性

使用江西 CA 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。

4.10 证书状态服务

4.10.1 操作特征

订户通过江西CA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

江西 CA 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。

4.11 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、备份与恢复的策略与行为

订户的签名密钥仅由订户的数字证书载体生成，加密密钥由密钥管理中心生成。

签名密钥由订户的数字证书载体保存。

密钥恢复是指加密密钥的恢复，签名密钥由订户自行保存，江西 CA 不接受订户签名秘钥的托管和恢复。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。订户向江西CA申请，经审核通过后，江西CA向密钥管理中心请求，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：司法取证人员在密钥管理中心申请，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与行为

会话密钥由非对称算法组织数字信封的方式封装，数字信封使用信息接受者的公钥对会话秘钥加密，接受者用自己的私钥解开并恢复会话秘钥，该密钥由订户的应用环境来决定使用，江西CA不对其进行保存和恢复。

5 认证机构设施、管理和操作控制

5.1 物理控制

系统的物理安全和环境安全是整个江西CA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。为把江西CA系统的危险减至最低限度，江西CA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。

江西CA系统中的基础设施包括涉及服务器、网络设备、安全设备、终端设备等资源的场所，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

江西 CA 主机房位于南昌市东湖区省府大院西二路 3 号。所有机房的建设和管理严格按照相关规定要求，采用高安全性的监控技术，包括视频实时移动监控、指纹、身份识别等技术，以确保物理通道的安全。核心区内墙六面全部用钢板焊接，屏蔽效果良好，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

江西 CA 机房只有经过江西 CA 授权的人员才能进入授权的工作区域。在进入江西 CA 机房时，必须经过身份识别。机房实行 7*24 小时自动监控。监控记录文件包括对机房通道上的所有踪迹的记录。江西 CA 的员工经授权后，至少两人才能进入机房。对于要进入机房的来访者，须经江西 CA 机房管理负责人批准后，指定江西 CA 的员工陪同。

江西 CA 按照安全级别划分为四个区域。分别是：公共区、服务区、管理区和核心区。通过公共区进入服务区、管理区以及核心区时，必须通过指纹验证和权限检验。在部分关键区域还采用 m of n 机制进行访问控制。

5.1.3 电力与空调

江西 CA 机房所在的楼内使用两路市电电源至 UPS 机房，公共区、服务区、管理区、核心区都配有足够容量的 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。

江西 CA 机房空调系统使用独立的空调和通风设备，保证温度、湿度处于可控的范围之内，以保证系统稳定的运行。

5.1.4 水患防治

江西 CA 机房内无渗水、漏水现象，主要设备采用专用的防水插座。机房内无上下水系统，机房管理人员每天巡查机房情况。

5.1.5 火灾防护

江西 CA 的机房建设和防护设施符合当地管理部门或机构的要求，机房内各区域均采用了温感和烟感火灾探测器，并安装了火灾自动报警系统及气体自动灭火系统，该系统具有自动和手动操作方式。在自动状态下，当防护区发生火警时，火灾报警控制器接到防护区火灾报警信号后立即发出联动信号。经过 30 秒时间延时，火灾报警控制输出信号，启动灭火系统，同时，报警控制器接收压力讯号器反馈信号，防护区内门灯显亮，避免人员误入。当防护区经常有人工作时，可以通过防护区门外的手动/自动转换开关，使系统自动状态转换到手状态，当防护区发生火警时，报警控制器只发出报警信号，不输出动作信号。由值班人员确认火警，按下控制面板或击碎防护区外紧急启动按钮，即可立即启动系统，喷发气体灭火剂。

江西 CA 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

江西 CA 的存储介质包括硬盘、光盘等，介质存储地点和江西 CA 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通过专业机构销毁，其他介质以不可

恢复原则进行相应的销毁处理。

5.1.8 异地备份

江西 CA 对系统重要数据进行定期备份，备份数据加密后刻录成光盘并保存于指定银行保险箱内，如遇灾难情况发生时保障了数据安全且用于灾后系统应急恢复。

5.2 程序控制

5.2.1 可信角色

江西 CA 提供的电子认证服务过程中，能从本质上影响证书的颁发、使用、管理和吊销等涉及密钥操作的职位都被江西 CA 视为可信角色。这些角色包括但不限于：密钥和密码设备的管理员、系统管理员、超级管理员、权限管理员、安全审计员、录入员、审核员等。

5.2.2 每项任务需要的人数

江西 CA 和 RA 根据各项敏感操作的安全要求规定所需的人员数量，即确保多个员工共同完成一项敏感操作。CA 密钥、相关加密设备以及机密文件的管理和操作应由多个可信人员共同完成且执行 m of n 机制（m≥2）。CA 及注册系统的日常维护操作应至少由 2 个信任人员完成。

5.2.3 每个角色的识别与鉴别

江西 CA 的可信人员，按照所担任角色的不同进行身份鉴别。进入机房需通过入口保安人员鉴别身份和两人以上指纹识别；进入系统需要使用数字证书进行身份鉴别。江西 CA 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，江西 CA 遵循可信角色分离的原则。系统管理员和安全审计员岗位不能由同一人担任；录入员和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

工作人员填写《江西 CA 个人简历表》及提供《无犯罪证明》，公司行政部对人员的资历、经历等情况进行核实，签订《劳动合同》及《保密协议》。

5.3.2 背景审查程序

江西 CA 对工作人员进行背景调查的程序符合法律法规的要求，调查内容、调查方式和从事调查的人员不会违反相关的法律、法规。

背景调查分为：基本调查和全面调查。基本调查包括对个人资历、工作经历等方面的调查。全面调查还包括对犯罪记录，社会关系等方面的调查。

背景检查程序为：

1、行政部对工作人员提供的资料进行审核，包括：个人履历、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。

5.3.3 培训要求

江西 CA 按照工作人员的岗位和角色安排不同的培训。培训内容有：

1、江西 CA 安全管理策略和机制；

2、PKI 基础知识；

3、身份认证和审核策略；

4、灾难恢复和业务连续性管理；

5、CP、CPS 政策及相关标准和程序；

6、电子认证服务的法律、法规及标准等需要培训的内容；

江西 CA 根据机构系统升级、策略调整等要求，不定期的对人员进行再培训。对于系统运营和安全策略管理人员，每年至少进行一次培训。

5.3.5 工作岗位轮换周期和顺序

对于可替换角色，江西 CA 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

当工作人员出现未经授权或超出权限使用江西 CA 系统等情况时，将立即对该名员工进行工作隔离。一经确认，将吊销该人员的登录证书、同时终止其系统访问权限，随后对该人员的未授权行为进行评估，并根据结果进行相应的处罚，情节严重的，将依法追究相应责任。

5.3.7 独立合约人的要求

对于不属于江西 CA 机构，但从事与江西 CA 业务有关的独立合约人，江西 CA 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、接受江西 CA 的上岗前培训及安全规范培训。

5.3.8 提供给员工的文档

为使得系统正常运行，江西CA向其员工提供完成其工作所必须的文档。

5.4 审计日志程序

5.4.1 记录事件的类型

江西 CA 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。包括但不限于：

1、订户证书生命周期管理事件，如：证书申请、更新、密钥替换、吊销等。

2、CA 密钥整个生命周期管理事件，如：密钥的产生、备份、存储、吊销、归档、销毁等。密码设备整个生命周期管理事件。

3、网络安全设备记录的日志及安全事件。

4、江西CA还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、其他按规定需要记录的内容。

5.4.2 处理日志的周期

江西CA每周对日志进行审查，并对审查日志的行为进行记录。

5.4.3 审计日志的保存期限

江西CA的审计日志保存到证书失效后七年。

5.4.4 审计日志的保护

江西CA执行严格的管理，确保只有江西CA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访问、阅读、修改和删除等操作。

5.4.5 审计日志备份程序

江西CA保证所有审计日志和审查总结都按照江西CA备份标准和程序进行备份。审计日志由系统管理员每周进行备份，采用在线和离线的备份工具。

5.4.6 审计日志收集系统

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；

网络通信系统；（包括防火墙等访问控制设备）

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。

5.4.7 对导致事件实体的通告

江西 CA 发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

江西CA有权决定是否对导致事件的实体进行通告。

5.4.8 脆弱性评估

江西CA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

江西CA对下列记录进行归档保存,包括但不限于：

1、江西CA的系统建设和升级文档

2、证书申请信息、证书服务批准和拒绝的信息、与证书订户的协议、证书和证书吊销列表

3、系统运行和认证服务产生的日志数据、认证系统证书密钥升级和更新信息等

4、电子认证服务规则、各类服务规范和运作协议、管理制度

5、系统数据库

6、人员进出记录和第三方人员服务记录

7、员工资料，包括背景调查、录用、培训等资料

8、各类外部、内部审查评估文档

5.5.2 归档记录的保存期限

所有归档记录的保存期一般规定证书失效后七年。在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。此外，在不违反法律法规和主管部门的规定的前提下，江西 CA 可以自主决定信息的存档期限，并且不需要对此做出说明和解释。

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。江西 CA 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。对重要数据，江西 CA 会采取同城异地备份的方式予以保存。

5.5.4 归档文件的备份程序

所有归档的文件和数据，保存在江西 CA 的主要存储场所。确有必要的，还将在同城异地保存其备份。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。只有授权的工作人员才能在监督的情况下，对档案进行读取操作。江西 CA 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。对于需要持续保存、归档的文件和数据，将根据江西 CA 的备份策略进行归档和整理。

5.5.5 记录时间戳要求

江西 CA 所有存档内容都有时间标识。对于纸质记录，由操作人员手工标注；对于电子记录，由系统自动标注，但这些时间信息未采用时间戳技术。

5.5.6 归档收集系统

由江西 CA 内部的工作人员或者具备安全控制措施的内部系统组成，依照人工记录和系统自动记录两部分进行产生和收集。并且由具备相关权限的人员进行管理和分类。

5.5.7 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。江西CA会定期验证归档信息的完整性。

5.6 电子认证服务机构密钥更替

当CA密钥对的累计寿命超过第6.3.2中规定的最大有效期时，江西CA将启动密钥更新流程，替换已经过期的CA密钥对。江西CA密钥变更按如下方式进行：

一个上级CA应不迟于其私钥到期之前60天停止签发新的下级CA 证书（停止签发日期）；

产生新的密钥对，签发新的上级CA证书；

在“停止签发证书的日期”之后，对于批准的下级CA（或最终订户）的证书请求，将采用新的CA密钥签发证书；

上级CA将继续利用原来的CA私钥签发CRL直到利用原私钥签发的最后的证书过期为止。

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，江西CA将按照灾难恢复计划实施恢复。

5.7.2 计算机资源、软件或数据的损坏

江西 CA 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，江西 CA 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

当江西 CA 根证书被作废时，江西 CA 应通知订户。当江西 CA 的根私钥被攻破或需要作废时，根据江西 CA 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

灾难发生后江西 CA 将在 24 小时内启动灾难恢复计划启用备用系统至少恢复以下业务：证书的签发、证书的吊销、发布证书吊销列表、OCSP 等服务，确保业务持续性。

5.8 电子认证服务机构或注册机构的终止

当江西 CA 及其授权服务机构需要终止经营时，将会严格按照《电子认证服务管理办法》第四章（第二十三条到二十七条）之规定执行。

6 认证系统技术安全控制

6.1 密钥对的生成和安装

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

CA 密钥对由国家密码主管部门批准和许可的密码设备生成并存放其中。密钥的生成、管理、存储、备份和恢复遵循主管部门的相关规定。用于此类密钥生成的密码模块必须通过国家密码主管部门鉴定、认证。

订户的签名密钥对由订户的密码设备（如智能 USB KEY 或智能 IC 卡等设备）

生成，加密密钥对由 KMC 生成。

6.1.2 私钥传送给订户

订户的签名密钥对由自己的密码设备生成并保存。

加密密钥对由 KMC 产生，通过安全通道传到订户的密码设备中。

6.1.3 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道，经注册机构传递到 CA。

订户的加密证书公钥，由 KMC 通过安全通道传递到 CA。

从 RA 到 CA 以及从 KMC 到 CA 的传递过程中，采用国家密码管理局许可的通讯协议及密钥算法，保证了传输中数据的安全。

6.1.4 电子认证服务机构公钥传送给依赖方

依赖方可以从江西CA的网站http://www.jxca.org.cn下载江西CA根证书，从而获得公钥。

6.1.5 密钥的长度

江西 CA 的电子认证服务系统支持签发 SM2 算法证书和 RSA 算法证书，SM2 证书密钥长度为 256 比特，RSA 证书密钥长度为 2048 比特。江西 CA 根据订户需求为订户签发不同算法类型和密钥长度的证书。

6.1.6 公钥参数的生成和质量检查

公钥参数的生成和质量检查必须使用国家密码主管部门批准许可的加密设备生成，例如由加密机、加密卡、USB Key、IC 卡等生成和选取，并遵从这些设备的生成规范和标准。这些设备内置的协议、算法等已经具备了足够的安全等级

要求。

6.1.7 密钥使用目的

订户的签名密钥可用于提供安全服务，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

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

接口安全：不执行规定命令以外的任何命令和操作；

协议安全：所有命令的任意组合，不能得到私钥的明文；

密钥安全：密钥的生成和使用必须在硬件密码设备中完成；

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

6.2.2 私钥多人控制（m 选 n）

为保证系统运营安全，对 CA 私钥的相关敏感操作采取多人协作方式，将私钥的管理权限分散到三组管理员手中，只有三组管理员均到场并得到许可的情况下，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订户的密钥设备保存，密钥管理中心不负责托管。

密钥管理中心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

订户的签名私钥江西 CA 和密钥管理中心都不备份。加密私钥由密钥管理中心备份，备份数据以密文形式存储确保加密私钥的安全。

6.2.5 私钥归档

江西CA的私钥经过加密后按照严格的安全措施保存。在私钥有效期结束后，仍将采取同样的安全保密机制进行保存，并遵从江西CA关于归档的规定。

6.2.6 私钥导入、导出密码模块

江西CA的私钥，严格的按照江西CA规定的程序和策略进行备份，备份必须分三个载体存储并由三人分别保管，恢复密钥时也由这三人依次插入备份载体导入进行恢复，除此之外的任何导入导出操作将不被允许。当 CA 密钥对备份到另外的硬件密码模块上时，以加密的形式在模块之间传送，并且在传递前要进行身份鉴别，以防止CA私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

江西CA不提供订户私钥从硬件密码模块中导出的方法，也不允许如此操作。

6.2.7 私钥在密码模块的存储

江西 CA 使用国家密码主管部门批准和认可的密码设备及密码模块进行私钥

存储，所有在密码模块中存储的私钥，都以密文的形式保存。

订户的私钥存储在符合国家密码管理规定的如USB Key等介质中，所有在这些介质中存储的私钥，都以密文的形式保存。对于使用软件密码模块生成的私钥，最好在硬件密码模块（如USB Key、IC卡）中存储和使用，也可以使用有安全保护措施的特定软件密码模块。

6.2.8 激活私钥的方法

江西 CA 默认，只有在通过密码验证后，方可激活私钥，除非订户自己进行变更，并愿意承担变更后的责任。对于存放在诸如订户USB Key 、智能卡、加密卡、加密机或者其它形式的硬件密码模块中的私钥，订户可以通过口令、指纹、IC 卡等方式进一步保护。当订户计算机上安装了相应的驱动后，将 USB Key 、智能卡等插入相应的设备中，输入保护口令或指纹，则私钥被激活。

江西 CA 的私钥存放于硬件加密模块中，其激活数据按照电子认证业务规则进行分割。必须经过三个被授权的人员共同操作，才能进行激活。未经授权的任何人员，不可以进行激活或者存取使用。

6.2.9 解除私钥激活状态的方法

江西 CA 解除私钥激活的方式为在其密码设备关闭的时候解除激活状态，或者具有私钥管理权限的管理员通过密钥管理程序，进行关闭激活私钥的操作。需要三名管理员同时在场。未经授权的任何人员，不可以进行相关操作。

订户解除私钥激活状态的方式由其自行决定，例如退出、切断电源、移开令牌/钥匙，自动冻结等。订户必须自行承担其解除私钥激活状态操作的风险和责任。

6.2.10 销毁私钥的方法

江西 CA 的私钥不再被使用，或者与私钥相对应的公钥到期或者被吊销后，加密设备必须被清空。同时，所有用于激活私钥的密码设备也必须被销毁或者收回。

订户的私钥不再被使用，或者与私钥相对应的公钥到期或者被吊销后，由订户决定其销毁方法，订户必须保证有效销毁其私钥，并承担有关的责任。

6.2.11 密码模块的评估

江西 CA 使用国家密码主管部门批准和许可的密码产品，接受其颁布的各类标准、规范、评估结果、评价证书等各类要求。江西 CA 根据产品性能、工作效率、供应厂商的资质等方面的评估，选择需要的模块。

6.3 密钥对管理的其它方面

6.3.1 公钥归档

公钥的归档，其操作过程、安全措施、保存期限以及保存策略和证书保持一致。归档要求参照本电子认证业务规则中 5.5 的相关规定。

6.3.2 证书操作期和密钥对使用期限

CA 证书的有效期不超过 20 年，订户证书有效期最长不超过 5 年 3 个月。

CA 密钥对使用期限和 CA 证书的有效期保持一致。订户证书的密钥对使用期限和订户证书的有效期保持一致。特殊情况下，对于签名类证书，为了验证在证书有效期内签名的信息，与之对应的公钥可以在证书的有效期限以外使用，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。

6.4 激活数据

6.4.1 激活数据的产生和安装

CA私钥的激活数据，必须按照关于密钥激活数据分割和密钥管理办法的要求，严格进行生成、分发和使用。

订户的激活数据包括下载证书的口令、用户密钥存储介质的PIN码等。下载证书的口令由江西CA在安全可靠的环境下随机产生，通过可靠的方式发送给订户。证书存储介质（如：USB_Key）出厂时设置有缺省PIN码，订户使用证书前，需重新进行设置。

江西CA建议用户自行进行修改，所有的保护口令都应该是不容易被猜到的，应该遵循以下几个原则：

（1）至少6位字符；

（2）至少包含一个字符和一个数字；

（3）至少包含一个小写字母；

（4）不能包含很多相同的字符；

（5）不能和操作员的名字相同；

（6）不能使用生日、电话等数字；

（7）用户名信息中的较长的子字符串。

6.4.2 激活数据的保护

对于CA私钥的激活数据，必须将激活数据按照可靠的方式分割后由不同的可信人员掌管，而且掌管人员必须符合职责分割的要求。

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。如果证书订户使用口令或PIN码保护私钥，订户应妥善保管好其口令或PIN码，防止泄露或窃取。如果证书订户使用生物特征保护私钥，订户也应注意防止

其生物特征被人非法获取。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。未授权用户尝试使用激活数据时，尝试达到预定的次数，激活数据会自动锁定。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

江西 CA 认证系统的信息安全管理，按照国家密码管理局公布的《证书认证系统密码及其相关安全技术规范》、工业与信息化部公布的《电子认证服务管理办法》，制定出全面、完善的安全管理策略和制度，在运营中予以实施、审查和记录。主要的安全技术和控制措施包括：身份识别和验证、访问控制、人员职责分权管理、网络访问控制、对系统登录密码进行定期修改。

6.5.2 计算机安全评估

江西 CA 的 CA 系统及运营环境通过了国家密码管理部门的安全测评和评审，并获得了相关资质。江西 CA 还将继续接受国家密码管理部门和上级主管部门的检查和评估，并根据检查结果对系统进行相关的改造和完善工作。

6.6 生命周期技术控制

6.6.1 系统开发控制

江西 CA 的系统由国家相关的安全标准和具有密码相关资质的可靠开发商开发，其开发过程符合江西 CA 系统管理的各项规定。

6.6.2 安全管理控制

江西 CA 电子认证服务系统的安全管理控制，严格遵循管理部门的有关运行管理规范和江西 CA 的安全管理策略进行操作。

江西 CA 认证系统的各项配置及任何修改和升级都会记录在案并进行控制，并且江西 CA 采用严格的管理体系来保证操作系统、网络设置和系统配置安全，以防止未授权的修改。

硬件设备从采购到上线前，会进行安全性的检查，用来识别设备是否被入侵，是否存在安全漏洞等。加密设备的采购和安装，在更加严格的安全控制机制下，进行检验、安装和验收。

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。

江西 CA 将根据安全需求的发展及行业发展动态，在不影响正常提供服务的前提下，积极采用先进的技术和设备，及时进行更新以保证系统生命周期的安全性。江西 CA 对系统的任何修改和升级都会记录在案并予以控制。

6.7 网络的安全控制

江西 CA 认证系统采用多级不同厂商防火墙和网络控制系统的保护，并且实施完善的访问控制策略。

认证系统只开放与申请证书、查询证书等相关的操作功能，供用户通过网络进行操作。

为确保网络安全，江西 CA 认证系统采取防火墙、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，以尽可能的降低来自网络的风险。

6.8 时间戳

江西CA电子认证服务系统的各种系统日志、操作日志都有相应的时间标识。这些时间标识不需要采用基于密码的数字时间戳技术。

根据对系统安全管理和控制的需要，江西 CA 会决定是否使用时间戳。根据不同数据对时间的敏感性、严密性和逻辑关系的要求，江西 CA 将确定时间戳服务的有关规范和策略。

7 证书、证书吊销列表和在线证书状态协议

7.1 证书

江西CA签发的证书符合ITU-TX.509V3：信息技术-开放系统互联-目录：认证框架标准；以及RFC5280：Internet X.509公钥基础设施证书和CRL结构。

7.1.1 版本号

江西CA签发符合 X.509 V3标准的数字证书，证书的版本信息存放在证书版本属性栏中。

7.1.2 证书扩展项

江西CA使用了标准扩展项和自定义扩展项，内容包括：

1、密钥用法（Key Usage e），此字段指示已认证的公钥有何种用途。

江西CA签发的订户证书根据证书类别可能包含以下密钥用法：

a) digitalSignature: 用于验证数字签名。

b) nonRepudiation: 用于提供抗抵赖服务的数字签名，这种服务防止签名

实体假拒绝某种动作中的证书。

c）keyEncipherment：加密密钥或其他安全信息，例如用于密钥传输。

d）dataEncipherment：加密用户数据，但不包括密钥或其他安全信息。

e）keyAgreement：用作公钥协商密钥。

f）keyCertSing：验证证书的 CA 签名。

g）CRLSign：验证 CRL 的 CA 签名。

i）decipherOnly：此项与 keyAgreement 一起使用时，公钥协商密钥仅用于加密数据。

2、基本限制（BasicConstraints）

用于鉴别证书持有者身份，如最终用户等。

3、增强型密钥用法（Extended Key Usage）

对于不同的证书，其增强型密钥用法可能包含以下几种：

a）服务器验证（1.3.6.1.5.5.7.3.1）

b）客户端验证（1.3.6.1.5.5.7.3.2）

c）代码签名（1.3.6.1.5.5.7.3.3）

d）安全电子邮件（1.3.6.1.5.5.7.3.4）

e）时间戳（1.3.6.1.5.5.7.3.8）

f）智能卡登录（1.3.6.1.4.1.311.20.2.2）

4、CRL 分布点（CRL Distrabution Point）

CRL 分布点包含可以获取 CRL 的 URL，用于验证证书状态。

5、自定义扩展

根据证书应用的不同，江西 CA 签发的订户证书中可能含有以下自定义扩展项：

1.2.86.11.7.1 个人身份标识号

1.2.86.11.7.2 个人社会保险号

1.2.86.11.7.3 组织机构代码号

1.2.86.11.7.4 工商注册号

1.2.86.11.7.5 企业国税号/地税号

7.1.3 算法对象标识符

江西 CA 签发的的 RSA 算法数字证书采用 SHA256WithRSAEncryption 签名算法，国 产 SM2 算法数字证书采用 SM3WithSM2Encryption 签名算法。

7.1.4 名称形式

江西 CA 签发证书的名称形式和内容符合 X.501 甄别名格式。

7.1.5 名称限制

订户证书的命名一定要有意义，可以通过名称确定证书主题中的个人、单位或者设备的身份，订户证书不应使用匿名或假名。在某些具有特殊要求的应用中，可以按照一定的规则为用户指定特殊名称，并且能够把该类特殊名称与一个确定的实体唯一的联系起来。

7.1.6 证书策略对象标识符

无规定

7.1.7 策略限制扩展项的用法

无规定。

7.1.8 策略限定符的语法和语义

无规定。

7.1.9 关键证书策略扩展项的处理规则

无规定。

7.2 证书吊销列表

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

7.2.1 版本号

X.509 V2。

7.2.2 CRL 和CRL 条目扩展项

无规定。

7.3 在线证书状态协议

江西CA为证书订户和依赖方提供OCSP（在线证书状态查询服务），OCSP为CRL的有效补充，方便证书订户和依赖方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、确认江西 CA 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。内部审计是由江西 CA 自己组织内部人员进行的审计，审计的结果可供江西 CA 改进、完善业务，内部审计结果不需要公开。外部审计由江西 CA 委托第三方审计机构来承担，审计的依据包括江西 CA 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，以及关国家或行业的相关标准。其频率可由江西 CA 决定或由法律制定的监管机构决定。

8.2 评估者的资质

江西CA的内部审计，由安全策略委员会组织各部门人员成立审计评估小组，由该小组完成内部审计工作。聘请的外部审计机构应具备以下资质：1）必须是经许可的、有营业执照的评估机构，在省内享有良好的声誉；2）了解信息安全体系、电子认证服务行业的有关技术、标准和要求。

8.3 评估者与被评估者的关系

内部审计：江西 CA 审计员与本机构的系统管理员、业务管理员、业务操作员等工作岗位不能重叠。

外部审计：外部评估者和江西 CA 之间是独立的关系，没有任何的业务、财务往来，或者其他任何利害关系足以影响评估的客观性。评估者就以独立、公正、客观的态度对江西 CA 进行评估。

8.4 评估内容

审计所涵盖的主题包括：

1、人事审查；

2、物理环境建设及安全运营管理规范审查；

3、系统结构及其运行审查；

4、密钥管理审查；

5、客户服务及证书处理流程审查。

8.5 对问题与不足采取的措施

对于内部审计结果中的存在的问题与不足，由江西 CA 审计评估小组负责监督相关的责任职能部门进行改进和完善，并提交改进总结报告。对于外部审计结果中所存在的问题和不足，江西 CA 将按照其工作报告进行整改，并接受再次审计和评估。

8.6 评估结果的传达与发布

除非法律明确要求，江西 CA 一般不公开评估结果。对江西 CA 关联方，将依据签署的协议来执行。

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

江西 CA 对证书订户收取证书签发和更新费用。证书订户有义务根据江西 CA 公布的价格或者与江西 CA 签署的协议中指明的价格向江西 CA 支付费用。

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，目前江西 CA 不收取查询费用。如果用户提出特殊需求，导致江西 CA 产生了额外的费用，江西 CA 将与用户协商收取应该收取的那部分费用。

9.1.3 证书吊销或状态信息的查询费用

对于证书吊销和状态查询，目前江西 CA 不收取任何费用。除非用户提出的特殊需求，需要江西 CA 支付额外的费用，江西 CA 将与用户协商收取应该收取的费用。如果证书吊销和状态信息查询的收费政策有任何变化，江西 CA 将会及时在网站 http://www.jxca.org.cn 上予以公布。

9.1.4 其它服务费用

江西 CA 可根据请求者的要求，订制其它服务。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，江西 CA 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，江西 CA 将不办理退证、退款手续。

9.2 财务责任

9.2.1 保险范围

目前，江西 CA 没有提供第三方保险服务。

9.2.2 其他资产

无规定。

9.2.3 对最终实体的保险或担保

目前，江西CA没有提供第三方保险服务。

9.3 业务信息保密

9.3.1 保密信息范围

江西CA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。

对于江西CA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，由江西CA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。

说明：

1、江西CA不保存任何证书应用系统的交易信息。

2、除非法律明文规定，江西CA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。江西 CA 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江西 CA 目录服务等方式向外公布。江西 CA 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

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。

当江西 CA 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 CPS 中具有保密性质的信息时，江西 CA 应按照要求，向执法部门公布相关的保密信息，江西 CA 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

江西 CA 尊重证书订户个人资料的隐私权，保证完全遵照国家对个人资料隐私保护的相关规定及法律。同时，江西 CA 将确保全体职员严格遵从安全和保密标准对个人隐私给予保密。

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，江西 CA 可通过目录服务等方式向外公布。

9.4.4 保护隐私的责任

江西 CA、任何订户、关联实体以及与认证业务相关的参与方等，都有义务按照本 CPS 的规定，承担相应的保护隐私信息的责任。当江西 CA 在任何法律法规或者法院以及公权力部门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，江西 CA 可以向特定对象公布相关的隐私信息，江西 CA 无须为此承担任何责任，而且这种披露不能被视为违反了隐私保护义务。

9.4.5 使用隐私信息的告知与同意

江西 CA 将采取适当的步骤保护证书订户的个人隐私，并将采取可靠的安全手段保护已存储的个人隐私信息，在未得到证书订户的许可之前，江西 CA 保证不会将隐私信息提供给无关的第三方（包括公司或个人），除了法律或政府的强制性规定之外。

9.4.6 依法律或行政程序的信息披露

除非符合下列条件之一，否则江西 CA 不会将订户的隐私信息提供给任何对象：

1、政府法律法规的规定并且经相关部门通过合法程序提出申请；

2、法院以及公权力部门处理因使用证书产生的纠纷时合法的提出申请；

3、具有合法司法管辖权的仲裁机构的正式申请；

4、证书订户以书面方式进行授权。

9.4.7 其他信息披露情形

如果证书订户要求江西 CA 提供某类特定客户支援服务如资料邮寄时，江西 CA 则需要把证书订户的姓名和邮寄地址等信息提供给第三者如邮寄公司。

9.5 知识产权

江西 CA 享有并保留江西 CA 提供的全部系统和软件的一切知识产权，包括所有权、名称权和利益分享权等。江西 CA 有权决定关联机构采用的软件系统，选择的形式、方法、时间、过程和模型，以保证系统的兼容和互通。江西 CA 签发的证书和提供的文档的一切版权、商标和其他知识产权均属于江西 CA 的产权，这些知识产权包括所有相关的文件和使用手册。授权发证机构在征得江西 CA 的同意后，可以使用相关的文件和手册。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

江西 CA 在提供电子认证服务活动过程中的承诺如下：

1）江西 CA 遵守《中华人民共和国电子签名法》及相关法律的规定，接受工业和信息化部的领导，对签发的数字证书承担相应的法律责任。

2）江西 CA 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）除非已通过江西 CA 发出了江西 CA 的私钥被破坏或被盗的通知，江西 CA 保证其私钥是安全的。

4）江西 CA 签发给订户的证书符合江西 CA 的 CPS 的所有实质性要求。

5）江西 CA 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）江西 CA 根据 CPS 及时吊销证书。

7）江西 CA 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，江西 CA 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

江西 CA 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江西 CA 的 CPS 的所有实质性要求。

2、在江西 CA 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，及时向江西 CA 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

订户一旦接受江西 CA 签发的证书，就被视为向江西 CA、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 CPS 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，可供江西 CA 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，订户应立刻通知江西CA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，应及时通知江西CA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CPS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CPS的有关条款。

9.6.5 其他参与者的陈述与担保

江西CA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CPS9.6.1中的明确承诺外，江西CA不承担其他任何形式的保证和义务。同时，江西CA将：

不保证证书订户、信赖方、其他参与者的陈述内容。

订户违反本CPS9.6.3之承诺时，或证书依赖方违反本CPS9.6.4之承诺时，得以免除江西CA之责任。

不对电子认证活动中使用的任何软件做出保证。

9.8 有限责任

根据《中华人民共和国公司法》、《中华人民共和国电子签名法》和其他法律法规的规定，作为依法设立的有限责任公司，江西 CA 只承担法律范围内的有限责任。

9.9 赔偿

江西 CA 及其授权的发证机构，对所有当事人（包括但不限于订户、申请者、接受者或信赖方）的合计赔偿责任，不可能超过如下所述对这些证书的封顶赔偿金额：对于有关一张特定证书的所有签名和交易处理的总计，江西 CA 及其授权的证书服务机构对于任何人（或者其它实体）有关该特定证书的合计赔偿责任应该限制在一个不超出下述数额的范围内（单位：人民币元）：

江西 CA 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；

机构个人证书：1000 元人民币；

机构证书：2000 元人民币；

设备证书：5000 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。江西 CA 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。

9.10 有效期限与终止

9.10.1 有效期限

本CPS自发布之日起正式生效。

9.10.2 终止

当新版本的CPS正式发布生效时，旧版本的CPS自动终止。在江西CA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

本CPS终止后，其效力将同时终止，CPS中的内容将视为无效使用，但对终止之日前发生的法律事实，CPS中对各方责任的规定及责任免除仍然适用。

9.11 对参与者的个别通告与沟通

江西CA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

经江西CA安全策略委员会授权，CPS编写小组每年至少审查一次本CPS，确保其符合国家法律法规和主管部门的要求及相关国际标准，符合认证业务开展的实际需要。本CPS的修改和更新，由CPS编写小组提出修订报告，经江西CA安全策略委员会批准后，由CPS编写小组负责组织修订，修订后的CPS经过江西CA安全策略委员会批准后正式对外发布，并送工业和信息化部备案。

9.12.2 通知机制和期限

本 CPS 在江西 CA 网站(http://www.jxca.org.cn)上发布。版本更新时，最新版本的 CPS 在江西 CA 的网站上发布，不做另行通知。

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

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

9.14 管辖法律

本 CPS 接受《中国人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》以及其它中华人民共和国法律法规的管辖和解释。

9.15 与适用法律的符合性

所有电子认证活动的参与方，都必须遵守《中国人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》以及其它中华人民

共和国法律法规的规定。

9.16 一般条款

9.16.1 完整协议

本CPS将替代所有以前的和同时期的条款。

9.16.2 转让

江西CA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

本CPS的任何条款或其应用，如果因为任何原因或在任何范围内发现无效或不能执行，那么本CPS其余的部分仍将有效。相关当事人了解并同意，本CPS所规定的责任限制、保证或其它免责条款或限制、或损害赔偿的排除等，均是可独立于其它条款的个别条款，并可加以执行。

9.16.4 强制执行

合同一方或几方不履行合同条款的，其它相关方可以依法要求强制执行。

可以声明在合同纠纷中有利的一方有权将代理费作为偿还要求的一部分，或者声明免除一方对合同某一项的违反应该承担的责任，但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

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，江西 CA 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

江西 CA 对本 CPS 拥有最终解释权。