四川 CA 电子政务电子认证业务规则

1.4 版本

版本说明：

四川 CA 电子政务电子认证业务规则版本控制表

版本	主要修订说明	生效时间	修订/批准
V1.2	新版本发布	2016 年 11 月 6 日	公司 CPS 编写小组/安全策略委员会
V1.3	1、修订“6.5.1.4 审计日志程序”中的“2 处理日志的周期”； 2、修订“6.5.2.2 私钥保护和密码模块工程控制”中的“2 私钥多人控制”； 3、修订“7.2.12 修订程序”； 4、修订“7.2.17 其他条款”。	2018 年 11 月 20 日	公司 CPS 编写小组/安全策略委员会
V1.4	1、 根据国家密码管理局新的要求和规范对原有表述进行了调整； 2、 修订对机构组织、个人身份的鉴别的内容； 3、 修订“证书的发布”相关内容； 4、 修订“证书补办”和“证书变更”相关内容； 5、 增加“CRL 备份及频率”； 6、其他内容表述的修订勘误。	2019 年 5 月 6 日	公司 CPS 编写小组/安全策略委员会

四川 CA 电子政务电子认证业务规则

四川省数字证书认证管理中心有限公司版权所有

目　录

1 概括描述

四川省数字证书认证管理中心有限公司（下称“四川省数字证书认证管理中心”，或简称“四川 CA”），为获得《电子认证服务使用密码许可证》和《电子认证服务许可证》的电子认证服务机构。

本文档的编制，遵从《中华人民共和国电子签名法》《电子政务电子认证服务管理办法》以及《电子政务电子认证服务业务规则规范》，阐明了四川 CA 面向电子政务活动中的政务部门和企事业单位、社会团体、社会公众等电子政务用户提供的证书申请、证书签发、证书更新、证书撤销以及密钥生成、备份和恢复等服务内容，以及相应的服务、法律和技术上的措施和保障，以供电子认证活动参与方了解和遵循。

本 CPS 详细阐述了四川 CA 签发和管理证书及运营维护证书服务设施的活动，并提供在实际工作和运行中遵循的各项规范。

本 CPS（v1.4 版本）的生效日期是 2019 年 5 月 6 日。

2 规则依据文件

本 CPS 的依据文件如下：

《中华人民共和国电子签名法》

《电子政务电子认证服务管理办法》

GM/Z 0001 密码术语

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0017 智能密码钥匙密码应用接口数据格式规范

GM/T 0018 密码设备应用接口规范

GM/T 0019 通用密码服务接口规范

GM/T 0020 证书应用综合服务接口规范

GM/T 0028 密码模块安全技术要求

GM/T 0034 基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范

GM/T 0054 信息系统密码应用基本要求

3 术语和定义

GM/Z 0001确立的以及下列术语和定义适用本文件

3.1 公钥基础设施 public key infrastructure（PKI）

基于公钥密码技术实施的具有普适性的基础设施，可用于提供机密性、完整性、真实性及抗抵赖性等安全服务。

3.2 加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.3 加密证书 encipherment certificate/exchange certificate

用于证明加密公钥的数字证书。

3.4 密码模块 cryptographic module

实现密码运算功能的、相对独立的软件、硬件、固件或其组合。

3.5 密码算法 cryptographic algorithm

描述密码处理过程的运算规则。

3.6 密钥 key

控制密码算法运算的关键信息或参数。

3.7 证书更新 Certificate update

指在不改变密钥的情况下，用一个新证书来代替旧证书的过程。

3.8 密钥更新 key update

用一个新密钥来代替旧密钥的过程，通常指证书与密钥同时更新。

3.9 密钥恢复 key recovery

将归档或备份的密钥恢复到可用状态的过程。

3.10 签名证书 signature certificate

用于证明签名公钥的数字证书。

3.11 身份鉴别/实体鉴别 authentication/entity authentication

确认一个实体所声称身份的过程。

3.12 数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

3.13 数字证书 digital certificate

也称公钥证书，由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.14 私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

3.15 SM2 算法 SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为256 比特。

3.16 证书撤销列表 certificate revocation list （CRL）

由证书认证机构（CA）签发并发布的被撤销证书的列表。

3.17 证书认证机构 certification authority（CA）

对数字证书进行全生命周期管理的实体。也称为电子认证服务机构。

3.18 证书注册机构 registration authority （RA）

受理数字证书的申请、更新、恢复和注销等业务的实体。

3.19 证书依赖方 certificate dependent

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证书持有者。

3.20 CA 注销列表 Certificate Authority Revocation list （ARL）

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。

4 符号和缩略语

下列缩略语适用于本规范：

CA	认证机构(Certification Authority)
CPS	证书业务声明（Certification Practice Statement）
CRL	证书撤销列表(Certificate Revocation List)
LDAP	轻量级目录访问协议(Lightweight Directory Access Protocol)
OCSP	在线证书状态协议（Online Certificate Status Protocol ）
RA	注册机构(Registration Authority)
LRA	证书注册受理点（Local Registration Authority）
ARL	认证机构CA证书的吊销列表（Certificate Authority Revocation list）

5 四川 CA《电子政务电子认证服务业务规则》管理规范

5.1 管理机构

四川 CA 安全策略委员会是本 CPS 的管理机构，负责组织起草 CPS，定期对存在的业务风险进行评估、并根据结果决定是否需要对 CPS 进行修订，并在服务范围公开发布；同时，四川 CA 安全策略委员会负责对 CPS 各版本的审核和批准工作，并监督 CPS 的执行。

5.2 联系方式

本《电子政务电子认证业务规则》在四川 CA 网站发布，对具体个人不另行通知。

四川 CA 网站：www.scca.com.cn

电子邮箱：cps@sicca.com.cn

联系地址：四川省成都市高新区交子大道 333 号中海国际中心 E 座 5 楼 509-512

联系部门：风控质量部

邮编：610041

电话：028-85336171

传真：028-85336171-808

5.3 批准程序

1、《四川 CA 电子政务电子认证业务规则》（CPS）由安全策略委员会指定相关人员组成 CPS 编写小组负责编写与修订。

2、CPS 由编写小组拟定并提交给安全策略委员会审核并批准。如需修订，由安全策略委员会指定相关人员进行修订，并负责向安全策略委员会提交修订内容，安全策略委员会审核并批准。

3、安全策略委员会审批通过后将最新的《四川 CA 电子政务电子认证业务规则》及时报国家密码管理局备案及进行归档，并以 PDF 格式在四川 CA 官方网站（www.scca.com.cn）上对外公布。

6 电子政务电子认证服务业务规范要求

四川 CA 电子政务电子认证服务严格按照《电子政务电子认证服务管理办法》所规定的服务内容及要求开展。

6.1 数字证书服务

6.1.1 服务内容

四川 CA 面向电子政务活动中的政务部门和企事业单位、社会团体、社会公众等电子

政务用户提供证书申请、证书签发、证书更新、证书补办、证书变更、证书撤销以及密钥生成、备份和恢复等证书全生命周期管理服务。

6.1.2 数字证书类型

四川 CA 提供以下类型的数字证书：

1） 机构证书

用以代表政务机关和参与电子政务业务的企事业单位、社会团体或其他组织的身份，如：代表单位和部门等机构身份证书。

2） 个人证书

为各级政务部门的工作人员和参与电子政务业务的社会公众颁发的证书，用以代表个体的身份，如：某局局长、某局职员或参加纳税申报的个人的身份证书等。

3） 设备证书

为电子政务系统中的服务器或设备颁发的数字证书，用以代表服务器或设备身份的真实性，如：服务器身份证书、IPSec VPN 设备证书等。

4） 其他类型证书

为满足电子政务相关应用的特殊需求而提供的其他应用类型的证书，如：代码签名证书等。

以上各类数字证书格式遵循 GM/T 0015，在标识实体名称时，保证实体身份的唯一性，且名称类型支持 X.500、RFC-822、X.400 等标准协议格式。

6.1.3 身份标识与鉴别

1 命名

电子政务数字证书命名遵循 GM/T 0015 的要求，不使用匿名或假名。

根据证书主体类型不同，四川 CA 签发的证书的主体名字可以是人员姓名、组织机构名、部门名、域名等，命名符合 X.501 甄别名规定。

运营设备证书的主体域中包含一个 X.501 甄别名，它的内容组成与服务器证书类似，只是其中的通用名(CN)对应的内容是设备的名称或 IP 地址，或者机构的名称。

2 证书申请人的身份确认

A. 证明持有私钥的方法

四川 CA 基于以下两个条件来证明证书持有者拥有私钥：

1）通过证书请求中所包含的数字签名来证明证书持有者持有与注册公钥对应的私钥。

a） 签名密钥属于证书申请者专有；

b） 证书申请者使用其私钥对证书请求信息进行数字签名；

c） 四川CA使用证书申请者公钥验证该签名。

2）证书私钥的保管符合GM/T 0034和GM/T 0028等相关标准规范。

B. 组织机构身份的鉴别

四川 CA 在把证书签发给一个组织机构或组织机构拥有的设备时，将对证书持有者所在的组织机构进行身份鉴别。对组织机构身份鉴别方式包括如下内容：

1）确认组织机构是确实存在的、合法的实体；

2）确认该组织机构知晓并授权证书申请，代表组织机构提交证书申请的人是经过授权的；

申请机构证书应提交组织机构成立的有效文件（如营业执照、统一社会信用代码证书等）及其复印件、经办人的有效身份证件、加盖公章的授权申请文件。

申请机构证书应提交符合填写规范的《机构证书申请表》。

四川 CA 的注册机构对上述材料进行审核和鉴证，作出批准申请或拒绝申请的操作。如批准申请，四川CA将保留相关证明材料的复印件及电子数据，与申请表一并存档保存，四川CA确保身份鉴别材料或电子数据具备不可篡改和抗抵赖性。

C. 个人身份的鉴别

在把证书签发给个人时，四川CA对证书持有者进行身份鉴别。对个人身份鉴别方式，包括如下内容：

1） 确认个人的身份是确实存在的、合法的实体；

2） 确认证书持有者知晓并授权证书申请，代表他人提交证书申请的人是经过授权的；

申请个人证书需提交合法身份证明文件及其复印件。合法的身份证明文件包括：身份证、户口簿、护照、军官证、警官证、士兵证、士官证和文职干部证等。

申请个人证书应提交符合填写规范的《个人证书申请表》。

四川CA对上述材料进行审核和鉴证，作出批准申请或拒绝申请的操作。

在把证书签发给政府部门个人时，还进行以下鉴证工作：

1）申请人提交加盖单位公章的证明文件，确保证书持有者所在的组织、部门与证书中所列的组织、部门一致，证书中通用名就是证书持有者的真实姓名；

2）确认证书持有者属于该组织机构，证书持有者确实被招录或聘用；

3）证书依赖方提供证书用户发放清单或提供证书发放用户库，四川 CA 通过辅助手段（如：短信、对公邮箱或公安部身份证库等）验证用户身份真实性。

四川 CA 对上述材料进行审核和鉴证，作出批准申请或拒绝申请的操作。如批准申请，四川 CA 注册机构保留相关证明材料复印件及电子数据，与申请表一并归档保存，确保身份鉴别材料或电子数据具备不可篡改和抗抵赖性。

3　密钥更新请求的识别与鉴别

A.　常规的密钥更新请求的识别与鉴别

对于一般正常情况下的密钥更新申请，证书持有者需要提交能够识别原证书的足够信息，并使用更新前的私钥对包含新公钥的申请信息签名。对申请的鉴别需满足以下条件：

1）密钥更新请求中，确保更新请求与申请者身份的关联和申请行为的有效性，采取现场受理点和远程在线等方式对用户身份进行实体鉴别。

2）申请对应的原证书存在并且由四川 CA 签发；

3）用原证书（有效期内的证书）上的证书持有者公钥对申请的签名进行验证；

4）基于原注册信息进行身份鉴别；

5）当用户证书已过期时，应重新进行与初始身份确认相同的鉴别流程；

6）当用户证书未过期时，用户采取在线更新方式的，由用户在线提交更新申请并进行数字签名，以实现对用户身份的实体鉴别。

B.　撤销之后的密钥更新请求的识别与鉴别

四川 CA 在证书撤销后不允许进行密钥更新。证书申请应重新进行与初始身份确认相同的鉴别流程。

4　撤销请求的身份标识与鉴别

在四川 CA 的证书业务中，证书撤销请求可以来自证书持有者，也可以来自四川 CA 或其注册机构。

证书撤销的方式可以是证书持有者自己撤销，也可以由证书持有者要求四川 CA 或其注册机构管理员撤销。

证书持有者通过四川 CA 或其注册机构申请撤销证书时，四川 CA 或其注册机构将对证书持有者进行身份鉴证。证书持有者申请撤销证书时，填写证书业务申请表，通过一定的方式，如面对面、邮寄、邮件、传真、在线申请等，向四川 CA 或其注册机构提交，并由四川 CA 或其注册机构审核。

四川 CA 或其注册机构的审核人员合理、审慎地核对申请资料的原件与复印件，根据审核人员的管理规定对申请者的资料的真实性进行审查，确认要撤销证书的人或组织确实是证书持有者本人或被授权人，并进行批准或拒绝的操作。

如果是因为证书持有者没有履行四川 CA 的电子政务电子认证业务规则所规定的义务，由四川 CA 或其注册机构申请撤销证书持有者的证书时，不需要对证书持有者身份进行标识和鉴别。

6.1.4 数字证书服务操作要求

6.1.4.1 证书申请

证书申请者提交证书申请时，需按照初始身份鉴别的要求，填写申请表，提交身份证明材料。

1 信息告知

四川 CA 在本 CPS 中阐述了受理证书申请的所有流程及要求，并通过网站、书面告知、现场咨询、电话、电子邮件等方式告知证书申请者及证书持有者所必须提交的材料和办理流程。

对于个人证书，申请者可通过在线、离线方式在四川 CA 网站或四川 CA 注册受理点填写数字证书申请表，并提供个人身份证明文件及其复印件一份，例如：身份证、军官证、学生证、护照、警官证、士兵证、士官证、文职干部证、及其他法律法规和政府政策认可的证明文件等。

政府、机构部门中的个人申请证书时，还需提交个人所在单位许可授权证明（申请表加盖单位公章）及单位证明文件；如果是委托申请的，还需提供经办人被授权证明，证明代表他人提交证书申请的人是经过单位授权的。

对于机构证书，申请者可通过线上、线下方式在四川 CA 网站或四川 CA 注册受理点填写数字证书申请表，申请者应提供单位对经办人的授权委托证明，单位的营业执照、统一社会信用代码证书及其他政府批文等有效证件，经办人的身份证和四川 CA 可能需要的其他文件。

任何需要在各类应用中采用数字证书进行真实身份标识和鉴别，实现信息保密，并提供信息源发性证明、完整性保障和抗抵赖的个人或机构，都可以申请个人证书或机构证书。

组织机构申请机构证书时，由机构授权人员申请。

服务器证书由域名拥有机构，或获得域名使用授权的机构中的授权人申请。

运营设备证书由四川 CA 授权的人员或者设备所在注册机构的授权人申请。

2　申请的提交

- 证书申请应由证书持有者或相应的授权人提交。
- 非证书持有者代表组织机构进行批量证书申请的还须获得该组织的授权。
- 四川 CA 提供线上、线下多种方式的证书受理申请。

3　注册过程与责任

证书申请者可到四川 CA 的注册服务站点、或其授权注册机构的注册服务站点，申请各类证书。

对于机构证书，注册时申请者须正确填写以下信息：

- 机构的真实身份标识信息，如机构法定名称、统一社会信用代码等；
- 机构授权的申请人信息，如姓名、电话、邮件地址等。

对于个人证书，注册时申请者须正确填写以下信息：

- 个人的真实身份标识信息，如个人真实姓名、身份证号码、电话号码、所属机构（若需要）等；
- 其他信息，如邮件地址等。

对于服务器证书和运营设备证书，注册时申请者须正确填写以下信息：

- 服务器主机名、域名、IP 地址、或设备名称、及所有者信息等；
- 申请人信息，如姓名、电话、邮件地址等。

四川 CA 在处理每一个证书申请中，满足以下条件：

- 保留对最终实体身份的证明和确认信息；
- 保证证书申请者和持有者信息不被篡改、私密信息不被泄漏；
- 注册过程保证所有证书申请者明确同意相关的证书申请者协议；
- 按本 CPS 的规定产生一个密钥对，并将使用私钥签名的证书注册请求通过网络安全传输协议传给四川 CA 或其注册机构。

证书持有者有责任向四川 CA 提供真实、完整和准确的证书申请信息和资料。

四川 CA 及其注册机构承担对证书持有者提供的证书申请信息与身份证明资料的一致性检查工作，承担相应审核责任；同时承担对申请材料保密的责任。

6.1.4.2　证书申请处理

1　执行识别与鉴别功能

对于个人证书的申请，四川 CA 或其注册机构按本 CPS 6.1.3 所述的方式对订户进行识别和鉴别。

对于机构证书和设备证书，四川 CA 或其注册机构按本 CPS 6.1.3 所述的方式对组织机构及其授权申请人进行识别和鉴别。

特别地，对组织机构代表人证书，除了对组织机构及其授权申请人进行识别和鉴别，还需确认包含在证书中的代表人个人信息是真实而准确的。

2　证书申请批准和拒绝

四川 CA 或其注册机构对申请信息及身份信息进行完整性、有效性、可靠性和真实性的鉴别，准确无误后，将批准该申请。

依据识别与鉴别的信息，四川 CA 或其注册机构有权决定接受或拒绝证书持有者的申请。如果符合下述条件，四川 CA 或其注册机构接受证书持有者的证书申请，为证书申请者办理证书签发服务：

1）成功标识和鉴别了证书持有者的身份信息；

2）申请者接受或者没有反对订户相关协议的内容和要求；

3）申请者按照规定支付了相应的费用，另有协议规定的情况除外。

如发生下列情形之一，四川 CA 或其注册机构有权拒绝证书持有者的证书申请，并在 2 个工作日内通过现场或者电话、邮件等方式告知拒绝原因：

1）该申请未能完成标识和鉴别；

2）申请者不能提供所需要的身份证明材料或其他需要提供的证明文件；

3）申请者不接受或者反对订户相关协议的内容和要求；

4）申请者没有或者不能够按照规定支付相应的费用；

5）四川 CA 或其注册机构认为批准该申请将会对四川 CA 或其注册机构带来争议、法律纠纷或者损；

6）上述原因之外，申请者没有在规定时间内响应、回复四川 CA 或其注册机构申请处理过程中发出的通知。

被拒绝的证书申请者可随后再次提出申请。

3　处理证书申请的时间

四川 CA 或其注册机构将在合理时间内完成证书请求处理。在申请者提交资料齐全且符合要求的情况下，处理证书申请的时间不超过 2 个工作日。

6.1.4.3 证书签发

1 证书签发中RA和CA的行为

在证书的签发过程中，四川 CA 的 RA 管理员负责证书申请的审批，并通过操作 RA 系统将签发证书的请求发往 CA 的证书签发系统。RA 发往 CA 的证书签发请求信息采用数字签名和数字信封的方式实现 RA 的身份鉴别与信息保密，确保请求发到正确的 CA 的证书签发系统。

四川 CA 的证书签发系统在获得 RA 的证书签发请求后，对来自 RA 的信息进行鉴别与解密，对于有效的证书签发请求，证书签发系统签发证书。

2 CA和RA通知证书申请者证书的签发

无论是拒绝还是批准证书申请者的证书申请，RA 将通过适当的方式通知证书申请者；如果证书申请获得批准并签发，RA 将通过适当的方式告诉证书申请者如何获取证书。

四川 CA 对订户的通告提供以下几种方式：

- 通过面对面的方式，通知订户（如到注册机构领取等方式）；
- 邮政信函通知订户；
- 通过电子邮件方式通知；
- 其他四川 CA 认为安全可行的方式通知订户。

6.1.4.4 证书接受

1 构成接受证书的行为

四川 CA 订户接受证书的方式可以有如下几种：

- 订户可通过面对面的方式，从注册机构（四川 CA 或其注册机构）接受载有证书和私钥的介质；
- 通过在线方式接受证书的，订户可根据获取证书的的指示信息，访问四川 CA 专门的证书下载服务站点将证书下载到本地存放介质，如 USB Key、智能卡等。安全要求符合 GM/T 0034 和 GM/T 0028 等相关标准规范；
- 订户按与四川 CA 约定的其他安全可靠方式获得证书的，并且没有提出反对证书或者证书中的内容；

完成以上行为表明证书持有者接受证书。另外，证书持有者接受到证书后，应立即对证书进行检查和测试。

2 CA对证书的发布

对于证书持有者证书，四川 CA 根据用户或证书依赖方的意愿将证书发布到目录系统上，对于明确表示拒绝发布证书信息的，四川 CA 不发布该证书信息；没有明确表示拒绝的，四川 CA 将证书信息发布到目录系统。

四川 CA 采用主、从目录服务器结构来发布所签发证书。签发完成的证书直接发布到主目录服务器中，然后通过主从映射，将主目录服务器的数据自动同步到从目录服务器中，供证书持有者和依赖方查询和下载。

3　CA对其他实体的通告

除证书持有者、证书申请者和 RA 外，四川 CA 不需要通知其他实体证书的签发。但使用证书的各类实体可以通过四川 CA 查询服务获得所需证书信息。

6.1.4.5　密钥对和证书使用

证书持有者的密钥对和证书须用于其规定的、批准的用途。签名密钥对用于签名与签名验证，加密密钥对用于加密解密。如果密钥对允许用于身份鉴别，则可以用于身份鉴别。密钥对和证书不应用于其规定的、批准的用途之外的目的，否则其应用是不受保障的。

1　证书持有者的私钥和证书使用

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撤销之后，订户必须停止使用该证书对应的私钥。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。订户应妥善保管其证书私钥。

2　依赖方的公钥和证书使用

当依赖方接受到经数字签名的信息后，应该，

- 获得数字签名对应的证书及信任链；
- 确认该签名对应的证书是依赖方信任的证书；
- 证书的用途适用于对应的签名；
- 使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。

当依赖方需要发送加密信息给接收方时，可以通过访问目录系统等方式获得接收方的公钥证书，然后使用证书上的公钥对信息加密。依赖方应将公钥证书连同加密信息一起发送给接收方。

6.1.4.6　证书与密钥更新

1　证书更新的情形

证书更新通常是指密钥不变，证书有效期延长，为证书持有者签发一张新证书。如果证书持有者的注册信息没有改变，证书持有者仅需提交能够识别原证书的足够信息，如证书持有者甄别名、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。

证书持有者必须在证书有效期到期前 60 天内，向四川 CA 或其注册机构申请证书更新。

若用户需要对原证书注册信息改变，四川 CA 将确认证书换发请求是被原证书持有者、证书持有者授权的代表或证书持有者所属机构提出的，并按本 CPS 6.1.3 对其进行鉴证，同初次申请流程办理。

证书到期或撤销后，将无法进行更新，只能按照初始流程重新申请证书。

2　请求证书更新的提交

证书持有者、证书持有者的授权代表（如机构证书等）或证书对应实体的拥有者（如设备证书等）在证书满足更新条件时，可以要求向四川 CA 的注册机构提出更新申请。

更新请求可采取当面提交更新申请或在线提交带有证书持有者数字签名的更新申请。

3　处理证书更新请求

对于不更换密钥的证书更新请求，用户提交的证书签名请求（PKCS#10）包含有原有证书的公钥，并由原证书私钥签名。

接收到用户的证书更新请求后，四川 CA 认证系统会自动完成如下验证操作：

1） 确认、验证申请对应的原证书存在并且由四川 CA 签发；

2） 证书更新请求在允许的期限内；

3） 用原证书上的订户公钥对更新申请的签名进行验证。

若以上自动验证通过，则四川 CA 或其注册机构根据证书种类的不同，分别按如下方式和过程完成证书更新请求的鉴证、批准，及新证书的签发：

对于机构证书（包括机构单位证书和机构代表人证书）和设备证书（包括服务器证书和运营设备证书）根据用户提交的原注册信息，按与新证书申请一样的流程完成证书申请的鉴别，包括机构身份信息正确性、有效性的验证和确认，证书申请人及证书申请授权的确认等。在进行鉴别时，若机构用户以前提交的机构身份证明文件（如营业执照）仍在其有效期内，则更新申请人无需重新提交有关的机构身份证明文件，但四川 CA 或其注册机构仍会通过第三方数据库确认有关材料是否继续有效。完成以上鉴别后，批准更新请求，签发新证书。

对于个人用户证书的更新，若包含在证书中的需鉴别的信息不包含该证书用户所属组织机构，则只要该证书用户履行了应尽的责任，则证书更新请求将获得批准，新证书将获得签发。若包含在证书中的需鉴别的信息包含该证书用户所属组织机构，则在批准更新请求、签发新证书前，需要确认该证书用户仍然是所属机构的人员。

对于机构雇员证书的更新，则在完成如下确认后，批准证书更新请求，签发新证书：

- 该证书用户仍然是对应机构的雇员；
- 该用户的证书更新获得了该机构的许可。

在以上验证和鉴别通过后才可进行证书更新，证书更新可以通过以下方式进行：

1）面对面的更新方式；

2）在线下载（成功）的方式。

4　通知证书持有者新证书的签发

同证书初次申请时的签发处理。

5　构成接受更新证书的行为

同证书初次申请时的接受规则。

6　CA 对更新证书的发布

同证书初次申请时的发布规则。

7　CA 通知其他实体证书的签发

同证书初次申请时的通知方式。

8　密钥更新的情形

密钥更新通常指密钥和证书同时更新，证书持有者申请密钥更新的情形有：

1）证书的密钥泄露或者损坏；

2）证书即将到期时，用户申请密钥更新；

3）当订户证实或怀疑其证书密钥不安全时；

4）其他四川 CA 认为有必要更换密钥确保证书安全等情形。

证书到期前 60 天起，如果用户希望继续使用证书、保持原有注册信息继续有效但要变更证书密钥对，可向四川 CA 或注册机构申请证书密钥更新。证书密钥更新将使用新的公钥但证书的签发者和主体名不变。

已过期或被撤销的证书不能进行密钥更新和证书更新，只能按照初始流程重新申请证书。

9　请求密钥更新的提交

同证书更新的处理。

10　密钥更新请求的处理

对于需要更换密钥的更新请求，四川 CA 或其注册机构将应对原证书、申请的签名信息及身份信息进行验证和鉴别，无误后方可进行。

鉴别过程同证书更新请求的处理。

11　通知证书持有者新证书的签发

同证书更新的处理。

12　构成接受密钥更新证书的行为

同证书更新的处理。

13　CA 对密钥更新证书的发布

同证书更新的处理。

14　CA 对其他实体的通告

同证书更新的处理。

6.1.4.7　证书补办

补办是指在证书有效期内，证书持有者出现证书载体丢失或证书载体损坏时进行证书补发的操作。补发操作成功时，旧证书将被撤销，新证书有效期从补发成功之日起到旧证书失效日止。证书补办业务的操作流程，按照初次证书申请的身份鉴别和受理流程执行。

过期证书和已撤销的证书无证书补办。

其他证书补办业务规则参照初次申请执行。

6.1.4.8　证书变更

有效期内的证书相关信息发生改变时（如机构组织名称、社会统一信用代码、姓名、身份证号等），用户须向四川 CA 申请对已签发的数字证书进行证书信息变更。变更操作成功时，旧证书将被撤销，新证书有效期从变更成功之日起到旧证书失效日止。证书变更业务的操作流程，按照证书申请的身份鉴别和受理流程执行。

过期证书和已撤销的证书无证书变更。

其他证书变更业务规则参照初次申请执行。

6.1.4.9　证书撤销

1　证书撤销的条件

四川 CA、注册机构及证书持有者在发生下列情形之一时，申请撤销数字证书：

A. 政务机构的证书持有者不从事原岗位工作；

B. 司法机构要求撤销证书持有者证书；

C. 证书持有者提供的信息不真实；

D. 证书持有者没有或无法履行有关规定和义务；

E. 四川 CA、注册机构或最终证书持有者有理由相信或强烈怀疑一个证书持有者的私钥安全已经受到损害；

F. 政务机构有理由相信或强烈怀疑其下属机构证书、人员证书或设备证书的私钥安全已经受到损害；

G. 与证书持有者达成的证书持有者协议已经终止；

H. 证书持有者请求撤销其证书；

I. 法律、行政法规规定的其他情形。

2 证书撤销的发起

当出现符合证书撤销条件中的情形时，以下实体可以请求撤销一个证书持有者证书：

A. 批准证书持有者证书申请的四川 CA、注册机构或证书使用唯一依赖方在满足证书撤销条件的前提下，可以要求撤销一个证书持有者证书。如存在证书一证通用的情形，其中某一个证书使用依赖方发起的证书撤销请求，该请求最终将由四川 CA 或其注册机构进行评估，决定是否接受撤销请求。

B. 对于个人证书，证书持有者可以请求撤销他们自己的个人证书。

C. 对于机构证书，只有机构授权的代表有资格请求撤销已经签发给该机构的证书。

D. 对于设备证书，只有拥有该设备的机构授权的代表有资格请求撤销已经签发给该设备的证书。

E. 司法机关等公共权力部门的授权代表可以要求撤销一个证书持有者证书。

3 证书撤销的处理

A. 四川 CA、注册机构在接到证书持有者的撤销请求后，通过核实身份证明材料，确认请求来自证书持有者本人或者得到了证书持有者的授权。

B. 对于验证通过的请求，在 CA 系统中执行撤销证书操作， 并在 24 小时内将撤销证书发布到证书撤销列表中。

C. 四川 CA、注册机构在确信出现证书撤销条件中的情况而需要立即撤销证书时， 可

以立即撤销证书。

D. 证书撤销后，通过现场当面、电子邮件、电话、传真等方式告知用户或依赖方证书撤销结果。

订户可以通过以下方式要求撤销自己的证书：

1） 直接访问四川CA或注册机构提供的证书服务网页，按照要求提交撤销请求及相关证明材料；

2） 现场提交撤销证书申请；

3） 通过电子邮件、电话、传真等可靠的方式告知四川CA或其注册机构。

4 依赖方检查证书撤销的要求

对于安全保障要求比较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：

A. 必须根据用户证书标明的发布地址获取四川 CA 的证书撤销列表，即 CRL。

B. 必须验证撤销列表的签名，确认其来自于四川 CA。

C. 必须验证证书撤销信息，确认用户证书是否被撤销。

5 CRL发布方式及频率

四川 CA 所有被吊销的证书列表 CRL，通过四川 CA 的目录服务器进行发布。至少在 24 小时以内发布一次订户证书的证书吊销列表（CRL），至少每年发布一次子 CA 证书（Sub-CA Certificate）的证书吊销列表（ARL），如果根证书被吊销，将及时在网站公布吊销信息。在某些特殊情况下，四川 CA 可自行决定公布证书吊销列表的时间和频率。

6 CRL发布的最大滞后时间

一个证书从它被撤销到它被发布到 CRL 上的滞后时间不超过 24 小时。

7 CRL备份及频率

四川 CA 对发布的 CRL 进行备份，最长时间间隔不超过 24 小时，备份保存时间不少于证书失效后 10 年。

8 在线状态查询的可用性

四川 CA 提供证书状态的在线查询服务（OCSP），该服务 7X24 小时可获得，服务地址、服务接口在通过与电子政务信息系统应用集成时，发布给电子政务信息系统调用。

9 在线状态查询要求

依赖方应检查证书的撤销状态。如果依赖方未通过 CRL 方式查询，则应通过 OCSP 在

线方式查询。

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：

A. 须按照查询协议要求，向 OCSP 服务地址提交状态查询请求；

B. 查询过程须确保信息传输的机密性和完整性；

C. 须获得证书状态信息。

10 撤销信息发布的其他形式

除了通过 LDAP 目录服务发布 CRL，或通过 OCSP 服务器提供证书状态查询外，四川 CA 所发布的 CRL 也可通过四川 CA 的相关服务网站获得。

6.1.4.10 密钥生成、备份和恢复

证书持有者的签名密钥对由证书持有者的密码设备（如智能密码钥匙 USBKEY 或智能 IC 卡）生成并保存，加密密钥对的生成、备份和恢复由四川省密钥管理中心提供密钥管理服务。

订户签名密钥对由证书持有者的密码设备保管。

加密密钥恢复是一种严格受控的过程，按照证书申请的身份鉴别与受理流程执行，将加密证书的归档或备份密钥，恢复到可用状态。只有在如下情况下才允许进行密钥恢复：

1 证书持有者提出申请：当证书持有者的密钥损坏或丢失后，某些密文数据将无法还原，此时证书持有者可申请密钥恢复。证书持有者到四川CA提交恢复申请，并注明原因；四川CA根据证书持有者的要求进行审核，审核通过后，四川CA再联系四川省密码管理局的密钥管理中心，由四川省密钥管理系统的业务管理员和业务操作员进行恢复操作，生成下载挑战码，提供给证书持有者；证书持有者访问RA用户服务页面使用挑战码下载证书。

2 国家执法、司法机构因执法、司法的需要，取证人员出示相关法律文件，向密钥管理中心提出恢复密钥的申请，经审核后，由四川省密钥管理系统的业务管理员和业务操作员进行恢复操作，生成加密密钥的密文文件，记录于特定载体中，提供给取证人员。

6.2 应用集成支持服务

6.2.1 服务策略和流程

四川 CA 提供的服务内容有：

1　制定证书应用实施的管理策略和流程，对业务系统进行充分调研，指导或参与业务系统证书应用部分的开发和实施；

2　制定项目管理制度，规范系统和程序开发行为；

3　制定安全控制流程，明确人员职责；

4　实施证书软件发布版本管理，并进行证书应用环境控制；

5　项目开发程序和文档等资料妥善归档保存。

6.2.2　应用接口

四川 CA 提供证书应用接口程序供应用系统集成和调用。

证书应用综合服务接口为上层提供简洁、易用的调用接口，符合 GM/T 0020 的要求，提供证书环境设置、证书解析、随机数生成、签名验证、加解密、时间戳以及数据服务接口等功能，并提供 C、C#、Java 等多种接口形态。除此之外，还涉及密码设备应用接口、密码模块安全技术接口和通用密码服务接口。

1　密码设备应用接口

密码设备应用接口包括服务器端密码设备的底层应用接口和客户端证书介质（如：USBKey）的底层应用接口。服务器端密码设备的底层应用接口在符合符合 GM/T 0018 的要求；客户端证书介质的底层应用接口符合 GM/T 0016 和 GM/T 0017 的要求。

2　密码模块安全技术接口

采用新模式与新技术密码模块安全技术接口，符合 GM/T 0028 和 GM/T 0054 的要求。

3　通用密码服务接口

通用密码服务接口为各类密码服务层和应用层提供统一的通用密码服务接口，符合 GM/T 0019 的要求。

6.2.3　证书应用方案支持

四川 CA 具备针对电子政务信息系统的电子认证安全需求分析能力、电子认证法律法规和技术体系的咨询能力以及满足业务要求的电子认证、电子签名服务方案的设计能力。

数字证书应用方案设计可包括：证书格式设计、证书交付、支持服务、信息服务、集成方案、建设方案、介质选型等。

6.2.4　集成内容

四川CA具备面向各类应用的证书应用接口集成能力，并达到以下要求：

1.　具备在多种应用环境下进行系统集成的技术能力，包括基于Java、.NET等B/S应用模式

和基于C、VC等C/S应用模式的系统集成能力。

2. 提供满足不同应用系统平台的证书应用接口组件包，包括com组件、java组件、ActiveX控件、Applet插件等。

3. 提供集成辅助服务，四川 CA 为电子政务应用单位提供证书应用接口程序集成工作。包括以下服务：

1) 证书应用接口的开发包（包括客户端和服务器端）；

2) 接口说明文档；

3) 集成演示 Demo；

4) 集成手册；

5) 证书应用接口开发培训和集成技术支持；

6) 协助应用系统开发商完成联调测试工作。

6.3 信息服务

6.3.1 服务内容

信息服务是面向证书应用单位提供证书发放和应用情况信息汇总及统计分析的信息管理服务。根据政务部门对证书应用信息的管理及决策需求，四川 CA 为证书应用单位提供以下信息服务，为其实现科学管理和领导决策提供可靠依据。

1 证书信息服务

四川 CA 的 CA 系统中签发、更新的数字证书，可实时或定时与电子政务信息系统进行数据同步，实现将证书信息同步到电子政务信息系统中。四川 CA 提交的数据包括业务类型、认证机构身份标识、用户基本信息、用户证书信息等。

2 CRL 信息服务

CRL 在 CA 系统中发布后，可实现将 CRL 实时发布到指定的电子政务信息系统中。四川 CA 提交的数据包括业务类型、认证机构身份标识、CRL 文件、同步时间等。

3 服务支持信息服务

四川 CA 面向电子政务用户、应用系统集成商、应用系统发布与之相关的服务信息，包括 CPS、常见问题解答、证书应用接口软件包等。

4 决策支持信息服务

四川 CA 面向电子政务应用单位、政府监管机构提供决策支持信息，包括用户档案信

息、投诉处理信息、用户满意度信息、服务效率信息等。

6.3.2 服务管理规则

1 四川CA内部工作人员按其工作角色设定与之相应的信息访问权限，并对其所有访问操作进行记录；

2 对证书应用单位的管理员设定信息访问权限，限定其仅能访问本应用所签发证书信息。

3 应用单位管理员对非授权信息的访问，须依照政策管理规定，须经上级主管部门批准后方可进行。

4 对问责程序需要进行的信息访问，四川CA严格审核相应的问责人员身份及授权文件， 无误后方可进行问责举证。

5 对监管部门应管理需求进行的信息访问，四川CA按照相关的管理规定和调取程序，为其提供信息访问权限。

6 对司法程序需要的信息访问，四川CA严格审核司法人员的身份及授权文件，确认后方可提供信息访问。

四川 CA 在提供信息服务时，确保做好相关信息的隐私保障机制，实现信息保护对用户的承诺。

1 私有信息类型的敏感度

以下信息属于私有信息：

A. 个人隐私信息；

B. 商业机密；

C. 政府部门的敏感信息和工作秘密。

证书申请过程中涉及的用户申请信息是敏感信息，而发布的证书和 CRL 信息不是敏感信息。证书发布根据用户要求进行公布与不公布。

2 允许的私有信息采集

四川 CA 仅在进行证书发行和管理时才收集本 CPS 声明的私有信息。除已与用户沟通确认外，四川 CA 不收集更多私有信息。

3 允许的私有信息使用

四川 CA 只使用 CA 或者 RA 收集的私有信息。

因在某项业务中开展证书应用而获得的私有信息，在使用时必须首先得到该业务应用

单位的许可。

4　私有信息的安全存储

四川 CA 将采取安全手段对用户私有信息进行安全存储，确保用户私有信息不发生泄露、未授权访问等安全事件。

5　允许的个人信息发布

四川 CA 和注册机构仅能面向证书应用单位发布与之相关的私有信息，以协助证书应用单位进行证书业务管理。

任何特定的私有信息发布均遵照相关法律和政策实行。

6　所有者纠正私有信息的机会

四川 CA 允许用户在其证书生命周期内对其私有信息进行更正。

7　对司法及监管机构发布私有信息

四川 CA 或者注册机构在以下情况下，可以执行将私有信息发给获得相应授权的人员：

A. 司法程序；

B. 经私有信息所有者同意；

C. 按照明确的法定权限的要求或许可。

6.3.3 服务方式

四川 CA 信息服务以页面或接口的形式向应用系统或证书用户提供服务，以接口形式提供的服务符合 GM/T 0020 的要求。

1　证书信息同步服务

证书信息同步服务通过采用 webservice 技术实现 CA 系统与电子政务信息系统的证书应用同步。电子政务信息系统通过部署统一的 webservice 接口，四川 CA 的 CA 系统通过调用统一的 webservice 同步接口，实现 CA 系统向电子政务信息系统进行证书信息的自动同步功能。同时，为了保证数据传输的安全性，通过对 webservice 通信数据添加数字签名，以防止数据在传输中被篡改或数据损坏。

2　CRL 信息同步服务

CRL 信息同步服务通过采用 webservice 技术实现 CA 系统与电子政务信息系统的 CRL 同步。 CA 系统主动调用该接口，实时将最新的 CRL 文件同步到电子政务信息系统中。为了提高 CRL 文件传输的安全性， 对发送的 CRL 数据进行数字签名，电子政务信息系统只需要根据认证机构身份标识找到对应的根证书链，验证 CRL 签名的有效性即可

确定 CRL 的有效性。CRL 发布周期不超过 24 小时。

3 服务支持信息服务

四川 CA 通过 WEB 网站面向电子政务用户发布如下信息：

- 电子政务电子认证服务业务规则；
- 证书生命周期服务流程及相关费用；
- 证书用户操作手册；
- 证书常见问题解答（FAQ）；
- 获得证书帮助联系方式（客服热线电话、办公地址、邮政编码、投诉电话等）。

四川 CA 通过 WEB 网站面向电子政务应用系统集成商发布如下信息：

- 数字证书应用接口软件包；
- 数字证书应用接口实施指南；
- 证书常见问题解答（FAQ）；
- 获得证书帮助联系方式（客服热线电话、办公地址、邮政编码、投诉电话等）。

四川 CA 通过 WEB 网站面向电子政务应用系统发布如下信息：

- 时间戳服务数据接口；
- http 协议的 CRL 发布服务接口；
- LDAP 协议的 CRL 发布接口；
- LDAP 协议的证书发布接口；
- OCSP 服务接口（可选）。

4 决策支持信息服务

四川 CA 面向应用提供方以 Web 或 WebService 方式提供如下信息服务：

- 用户档案信息：分业务、地域、时段等要素提供用户信息的统计分析服务；
- 投诉处理信息：提供特定业务、时间、特定用户群、问题类型等的投诉处理汇总信息及分析；
- 用户满意度信息：提供面向业务的用户满意度调查信息；
- 服务效率信息：提供面向业务的服务效率分析信息，如处理时间、服务接通率等。

6.4 使用支持服务

6.4.1 服务内容

使用支持服务是四川 CA 面向证书使用用户（即证书申请者、证书持用者）及证书应

用单位提供的一系列售后服务及技术支持工作。

服务内容包括：数字证书管理、数字证书使用、证书存储介质使用、电子认证软件系统使用、电子认证服务支撑平台使用以及各类数字证书应用（如证书登录、证书加密、数字签名）等贯穿证书使用和应用过程中的所有问题。

1　面向证书持有者的服务支持

A. 数字证书管理

包括数字证书的导入、导出，以及客户端证书管理工具的安装、使用、卸载等。

B. 数字证书应用

基于数字证书的身份认证、电子签名、加解密等应用过程中出现的各种异常问题，如：证书无法读取、签名失败、证书验证失败等。

C. 证书存储介质硬件设备使用

包括证书存储介质使用过程中出现的口令锁死、驱动安装、介质异常等。

D. 电子认证服务支撑平台使用

为用户提供在四川 CA 的数字证书在线服务平台中使用的各类问题，如：证书更新失败、下载异常、无法提交撤销申请等。

2　面向应用提供方的服务支持

A. 电子认证软件系统使用

提供受理点系统、注册中心系统、LDAP、OCSP、信息服务系统等系统的使用支持问题，如证书信息无法查询、数据同步失败、服务无响应等。

B. 电子签名服务中间件的应用

解决服务中间件在集成时出现的各种情况，如客户端平台适应性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等。

6.4.2 服务方式

四川 CA 提供多种服务方式，不断满足用户需求，提升用户满意度，包括不限于座席服务、在线服务、现场服务等，用户可通过四川 CA 网站等渠道获取服务方式。

四川 CA 建立了服务保障体系，包括建立专业的服务队伍、服务规范、知识库、服务跟踪系统、满意度调查、投诉受理等。服务保障体系能根据服务业务的变化及时更新。

1　座席服务

用户拨打四川 CA 的服务热线，通过语音系统咨询证书应用问题，热线坐席根据用户

的问题请求，查询系统知识库清单，协助用户处理。

2　在线服务

在线服务通过提供自助信息查询系统、远程终端协助系统，以及在线帮助与传统模式的结合，满足用户多种服务帮助的需求。

A. 自助信息查询系统

将知识库信息按照不同的类型、属性、层次等方式、结构进行分类存储，用户可以按照咨询问题或者已知条件在信息系统上进行启发式的检索，查找目标问题的答案。

B. 网络实时通讯系统

用户通过在线帮助网站远程发起支持请求，四川 CA 客服人员能够第一时间同登陆网站的访客取得联系，进行交流。

C. 远程终端协助系统

用户通过安装远程终端软件，可以通过互联网向客服人员发起协助请求。由服务人员通过远程终端控制功能，实时检测用户的软硬件环境，通过同屏显示指导、帮助用户解决应用故障。

D. 在线帮助与传统模式的结合

将在线服务系统与电话服务结合，方便用户既可以打电话、也可以自助上网，随时查询自己的服务记录、请求处理状态、产品配置信息等等。

3　现场服务

根据用户的实际需求， 由技术支持工程师上门现场为用户处理数字证书应用中存在的问题。

4　满意度调查

通过多种用户可接受的调查方式进行用户回访，包括电话、WEB 网站、邮件系统、短信、传真等。向用户提供调查表格以供用户填写， 调查表格清晰载明此次回访的目的及内容。并将用户回访中产生的相关文档进行归档、保存。

5　投诉受理

向用户公布电子政务电子认证服务监管部门的投诉受理方式。可通过电话、网站平台、电子邮件、即时通讯工具等方式及时接受用户投诉，投诉受理过程中记录投诉问题，并将结果及时反馈给用户。将投诉受理中产生的相关文档进行归档、保存。

6　培训

四川 CA 提供全面的培训服务，包括：电子认证服务基础性技术知识、服务规范、证书应用集成规范及相关帮助文档、常见问题解答(FAQ)、操作手册等。

培训方式可以由四川 CA 与用户双方约定的形式开展。

6.4.3 服务质量

四川CA提供的服务方式，包括不限于座席服务、在线服务、现场服务等，用户可通过四川CA网站等渠道获取服务方式。

四川 CA 的座席服务、在线服务、现场服务时间充分满足各类用户的需要，为 5X8 小时工作时间，热线电话服务时间是 7X24 小时不间断服务。在有应急服务需求的特殊情况下，服务时间根据具体业务需求确定，提供 7X24 小时不间断服务。

四川 CA 设有专门的投诉受理热线，按照投诉事件进行分级，承诺投诉处理不超过 1 个工作日。

为用户提供培训服务的同时，四川 CA 制定了用户培训意见反馈表，对培训效果进行评估，并做出相应处理，保证优质的培训效果和客户服务质量。

四川 CA 将技术问题和技术故障按照一般事件、严重事件、重大事件进行分类，并制定相应处理流程和机制，以确保服务的及时性和连续性。技术支持响应时间以最大程度不影响用户使用为准则。

6.5 安全保障

6.5.1 认证机构设施、管理和操作控制

6.5.1.1 物理控制

1 场地区域与建筑

四川 CA 认证业务的运营场地是按照 GM/T 0034 的要求严格实施，具有相关屏蔽、消防、物理访问控制、入侵检测报警等相关措施，至少每 5 年进行一次屏蔽室检测。整体建筑由能够阻止物理入侵的材料建成。建筑物的外墙、地板和天花板都属于永久性建造，并互相联结，可以阻止未经过授权的进入、入侵。敏感区域只设置一个门作为常规入口。根据消防要求设置了消防紧急出口。

运营场地的物理安全是基于物理层级的保护，每一物理层就是一个屏障，设置了门禁控制系统来控制每个人进出每一个区域。每一层区域有非常严格的控制方法防止未经授权的物理访问，而且每一个物理安全层在物理上完全包含下一个物理安全层，最外层的安全层是整个建筑物的外墙。

四川 CA 的运营场地达到以下安全和控制风险要求：

- 防止未经过授权的物理访问

确保未经过授权的人，或仅被授权访问有限物理区域的人员，不得访问四川 CA 内的受限制区域。

- 维护 CA 服务的完整性、可用性

保障提供 CA 服务的系统、设施不受到破坏，保证认证服务不被中断。

2　物理访问

四川 CA 物理设施的门禁系统实现了以下安全功能：

- 系统采用身份识别卡和生物识别鉴定的控制方法，控制每道门的进出；
- 授权人员进出每一道门都会有时间记录和相关信息提示；
- 所有的门都设有强行开启报警；
- 高敏感区域安装了移动报警器，防止任何未经允许的人员滞留在房间内；
- 整套访问控制系统配有断电保护装置，还配有发电机、UPS 提供紧急用电。

与门禁系统配合使用的还有录像监控系统，所有的录像资料根据安全审计要求保留一段时间。

3　电力与空调

四川 CA 有安全、可靠的电力供电系统及电力备用系统以确保系统 7X24 小时正常供电及在出现供电系统出现供电中断是能够提供正常的服务。四川 CA 机房的 UPS 系统为两台 400KVA 的 UPS 机组并联使用，完全停电时可支持设备使用近 8 小时。另外，机房所在大厦配有连接发电机的线路，可为机房提供外接发电机供电方式。

四川 CA 还具有新风/空调系统控制运营设施中的温度和湿度。

4　水患防治

四川 CA 机房内安装有专门的漏水报警装置，以及时检测漏水情况的发生。

5　火灾预防和保护

1）结构防火

四川 CA 的运营中心耐火等级符合 GBJ45《高层民用建筑设计防火规范》中规定的二级耐火等级，防护方法符合当地管理部门或机构的安全要求。

2）火灾报警及消防设施

四川 CA 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。

敏感区及高敏区配置了独立的气体灭火装置。

3）紧急出口

根据国家的有关消防要求、规定和标准，在非敏感区及敏感区的办公区域内，设置了紧急出口，紧急出口设有消防门。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。紧急出口门外部没有门开启的装置，且紧急出口门与门禁报警设备联动外。非紧急避险状态下，紧急出口门不能被内部人员任意打开。

6　介质存储

四川 CA 对储存产品软件和数据、归档、审计或备份信息的介质保存在安全设施中，这些设施受到适当的物理和逻辑访问控制的保护，只允许授权人员的访问，并防止这些介质受到意外损坏（如水、火灾和电磁）。

7　废物处理

四川 CA 对敏感的文件和材料在处理之前将其切成碎片，使信息无法恢复。密码设备在作废处置前根据制造商的指南将其物理销毁或初始化。其他废物处理按四川 CA 正常废物处理的要求进行。

8　异地备份

四川 CA 对关键系统数据、审计日志数据和其他敏感信息进行日常备份，这些备份信息保存在四川 CA 建筑物以外的安全的地方。

9　入侵侦测报警系统

四川 CA 在机房场所建筑区域内安装入侵侦测报警系统，进行安全布防，安装有移动侦测器报警器，发生非法入侵时能立即报警。

6.5.1.2 操作过程控制

1　可信角色

为了保证可靠的人员管理，保证证书服务具有高可靠性和高安全性，四川 CA 对关键岗位人员定为可信角色，四川 CA 可信人员包括：

- 技术研发人员
- CA 系统运行维护人员
- 网络维护人员
- 系统维护人员

- 核心机房管理人员
- 物理环境安全管理人员
- 安全策略委员会主任
- 安全经理
- 密钥管理人员
- 系统审计人员
- 可信雇员管理人员
- 录入与审核人员
- 用户档案管理人员

2　每项任务需要的人数

四川 CA 有严格策略和控制程序，以保障基于工作性质的职责分离。最敏感的操作要求多名可信人员共同参与完成。

- 鉴证和签发机构证书和管理员证书，要求 2 个可信人员的参与。
- 访问屏蔽机房需要至少两名有访问权限的人员。
- CA 秘密共享持有者采用 3 of 2 的控制方式。
- 操作存放有 CA 密钥的密码设备，至少需要一名操作员，一名见证人。

3　每个角色的识别与鉴别

对于物理访问控制，四川 CA 通过门禁磁卡、指纹识别鉴别不同人员，并确定相应的权限。

对于进行证书生命周期管理的四川 CA、注册机构证书管理员，他们使用相应的数字证书访问认证系统、注册机构系统，完成证书管理工作。

对于系统维护人员，他们使用安全的身份鉴别机制进入认证系统进行维护工作。

4　需要职责分割的角色

所谓职责分割，是指如果一个人担任了完成某一职能的角色，就不能再担任完成另一特定职能的角色。四川 CA 对如下人员进行了职责分割：

- 数据库管理员与应用系统管理员和操作系统管理员
- 操作员与审计员
- 审计与运维人员
- RA 业务录入与审核人员

6.5.1.3 人员控制

1 资格、经历和无过失要求

在四川 CA 中担任一定角色、执行一定功能、完成一定工作的人员，其所受教育、培训及工作经历足够胜任其工作。

四川 CA 客服人员必须受过专门的客服技能培训，通过 PKI 及相关应用基本知识培训，熟悉有关证书业务，考试通过后方能进行有关工作。这些培训和考试由四川 CA 负责。

四川 CA 安全管理人员必须熟悉、掌握有关的安全知识和安全管理，熟悉四川 CA 安全要求，熟悉四川 CA 安全与审计指南，有很强的责任感。为了达到此要求，四川 CA 将对安全管理人员进行培训。

四川 CA 密钥与密码设备管理人员必须熟悉 PKI 基本知识，熟悉 CA 证书和密钥相关的证书，如 CA 证书的产生、签发、更新、密钥更新等，熟悉有关密码设备操作使用。

四川 CA 所有的可信人员必须符合清白要求：没有伪造教育、工作经历，没有违法犯罪记录，工作中没有严重的不诚实行为。

2 背景审查程序

为了确保担任可信角色的人员能够胜任有关工作，四川 CA 将按照《四川 CA 可信雇员政策》对雇佣的人员先进行背景调查。在成为四川 CA 的可信人员前，有关人员必须提交相关材料，以证明他们能够胜任预期的工作。

四川 CA 依据有关材料进行背景调查，在调查过程中，四川 CA 将为有关人员保密，保护其隐私。

背景调查时如果出现提交材料与事实不符或证明提交材料为捏造时，四川 CA 将拒绝可信职位候选人获得有关职位或取消其可信人员的资格。

3 培训要求

为了使有关人员能胜任其承担的工作，四川 CA 对所有入职员工提供专门的培训计划，培训内容包括：

- 本人工作职责；
- 公司制度、流程，CPS；
- 岗位工作职责、流程；
- 电子认证相关法律法规；
- 安全管理要求及制度；

- 运营管理体系；
- 事故和安全威胁的报告和处理。

对于客服和系统维护人员还包括：

- PKI 及应用；
- 四川 CA 的产品与服务；
- 客服流程与要求（用户服务）；
- 安全操作流程（系统、密钥）。

4　再培训周期和要求

根据四川 CA 策略调整、系统更新等情况，四川 CA 要求员工根据情况及时进行继续培训，以适应新的变化。相关人员每年至少进行 1 次公司安全管理策略、相关技能知识的培训。

5　工作轮换周期和顺序

根据业务发展和运营管理需要，四川 CA 会根据岗位适应性和可替换角色，选派适当的人员进行不同岗位的轮换。岗位轮换不违背岗位分离原则。

6　对下列行为的处罚

四川 CA 对于未授权行为、未授予的权力使用、对系统的未授权使用或其他违反公司安全策略和程序的行为制定有相应的处罚措施，包括警告、罚款直至辞退，情节严重的将依法追究刑事责任。

7　独立合约人的要求

针对四川 CA 人力资源不足或特殊需要，聘请专业的第三方服务人员参与系统维护、设备维护等，除了必须就工作内容签署保密协议外，该服务人员必须在四川 CA 专人全程监督和陪同下从事相关工作。同时还需要对其进行必要的知识培训和安全规范培训，严格遵守规范执行。

8　提供给员工的文档

提供给员工的文档通常包括员工培训资料及员工工作手册等。

6.5.1.4 审计日志程序

1 四川 CA 建立了明确的审计日志程序：

- 确定CA 中心的业务符合对CPS 等文档中的定义；

- CA 中心的管理人员需要定期对安全策略和操作流程的执行情况进行检查确认，进行运营风险评估；
- 必须准确完整地记录CA 机构涉及运营条件和环境、密钥和证书生命周期管理的日志和事件；
- 各类日志、安全事件的记录在安全和公正的情况下以自动或手动方式产生，并定期归档。授权安全管理人员定期检阅记录和跟进有关事项；
- 建立监测 CA 系统访问的检测系统，保证非授权的访问能够被发现。

2 处理日志的周期

对于上述事件日志记录，四川CA每两个月进行一次内部检查、审计。

3 审计日志保存期限

与证书相关的审计日志，在证书失效后至少保留5年。

4 审计日志的保护

四川CA采取了物理和逻辑的访问控制方法，防止未经授权而浏览、修改、删除或其他方式篡改电子或纸质审计日志文件。

5 审计日志备份程序

对于认证系统的日志，四川CA定期进行备份。

6 审计收集系统

对于电子审计信息，四川CA自动或人工完成审计信息的收集。对于纸质的审计信息，则有专门的文件柜来存储。

7 对导致事件主体的通知

四川CA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。

8 脆弱性评估

对在审查过程中发现的系统的脆弱性，四川CA的关键人员，包括审计管理员、安全管理员、系统超级管理员等，或者聘请专业的系统安全评估单位，共同进行相应的脆弱性评估，出具评估报告，并在要求期限内对系统脆弱性进行修补。

对在审查过程中发现的物理安全、制度安全、人员安全等方面问题，及时进行相应的处理和解决。

6.5.1.5 规定事件记录的类型

四川 CA 对如下几类事件进行记录：

1. 对注册系统和证书受理操作的相关授权记录及管理记录：

- 证书的申请、批准、更新、撤销等；
- 成功或失败的证书操作；
- 证书系统用户权限的创建、删除、设置或修改密码。

这些记录由认证系统自动记录，保存在数据库。

2. 对证书、密钥、密码设备和 CRL 等生命周期的操作与管理进行事件记录：

- 证书签发和 CRL 列表生成记录：由认证系统自动记录，保存在数据库；
- 密钥生成，备份，存储，恢复，归档和销毁；
- 密码设备生命周期的管理事件，例如接收、使用、归档和销毁。

CA 密钥相关管理记录由密钥管理员进行纸质记录。

3. 对 PKI 系统的配置与操作进行事件记录：

- 系统登录、退出：由系统自动记录，保存在系统日志或数据库，由系统维护人员定期检查；
- 系统配置变更记录：由系统管理员进行纸质记录。

4. 系统崩溃、硬件故障和其他异常等进行事件记录：

- 成功或不成功访问 CA 系统的活动；
- 系统启动和关闭；
- 系统崩溃，硬件故障和其他异常。

这些记录由操作系统自动完成，由系统维护人员定期检查。

5. 对系统网络以及安全设备的日常运维操作进行事件记录：

- 路由器、防火墙等安全设备记录的安全事件；
- 对于 CA 系统网络的非授权访问及访问企图。

这些记录由网络和安全设备自动记录，由网络安全维护人员定期检查。

6、物理设施的访问记录：

- 授权人员进出；
- 非授权人员进出及陪同人。

授权人员进出物理设施由四川 CA 物理场地的访问控制系统自动记录。非授权人员

进出由陪同人员作纸质记录。

7、可信人员管理记录，包括且不限于，

- 网络权限的帐号申请记录；
- 系统权限的申请、变更、创建申请记录；
- 人员情况变化。

6.5.1.6 规定事件记录的内容

事件记录包括：事件类型、发生时间、相关内容，以及操作身份的实体；

PKI 系统的审计事件记录通过数字签名或由审计员专人备份等方式确保不能被篡改。

6.5.1.7 记录归档

1 归档记录的类型

四川 CA 对所有审计数据、证书申请信息、支持证书申请的文档等进行归档处理。

2 归档记录的保存期限

对于不同的归档记录，其保留期限是不同的。对于系统操作事件和系统安全事件记录，其归档保留到完成安全脆弱性评估或一致性审计。

- 面向企事业单位、社会团体、社会公众的电子政务电子认证服务，信息保存期为证书失效后 5 年；
- 面向政务部门的电子政务电子认证服务，信息保存期为证书失效后 10 年；
- 对 CA 证书和密钥生命周期内的管理事件的归档，其保留期限不少于 CA 证书和密钥生命周期；
- CA 证书和密钥的归档在 CA 证书和密钥生命周期之外，额外保留 10 年；
- 对系统操作、物理场地访问、可信人员管理记录的保存期限不少于 1 年。

3 归档文件的保护

四川 CA 对各种电子、纸质形式的归档文件，都有安全的物理和逻辑保护措施和严格的管理程序，确保其安全和保密，防止非授权的访问、修改、删除或其它的篡改行为。

4 归档文件的备份程序

所有纸质归档记录由专人定期进行归档和备份，电子存档文件由四川 CA 定期备份。

5 记录时间戳要求

四川 CA 对每项日志有时间记录。对于纸质记录，有操作人员手工记录；对于电子记录，由系统自动增加时间。

6　归档收集系统

四川 CA 档案收集由人工操作和自动操作两部分组成。

7　获得和检验归档信息的程序

只有可信人员才可以查看和获得归档信息，这些信息被归还时必须得到检验。

6.5.1.8 认证机构密钥更替

当 CA 密钥对的累计寿命超过规定的最大生命期，四川 CA 将启动密钥更新流程，替换已经过期的 CA 密钥对。

1　CA 根密钥更替：

- 采取与系统原根密钥初始化生成相同的流程和方法；
- 在新旧根证书过渡期，采用新私钥为旧公钥签名证书、旧私钥为新公钥签名证书、新私钥为新公钥签名的证书方式，保证用户和依赖方能够可靠地验证 CA 根证书以及确保证书信任链的有效性。

2　在线运营 CA 密钥更替：

- 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 或最终用户证书请求，将采用新的 CA 密钥签发证书；
- 上级 CA 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。

“停止签发日期”指：一个上级 CA 将在其私钥到期时间小于下级 CA 的生命期之前停止签发新的下级 CA 证书。

6.5.1.9 数据备份

四川 CA 建立了业务连续性计划和严格的备份管理策略，定期开展数据备份。

同城数据备份采用磁盘阵列、双机容错、在线实时备份等多种方式处理数据，具备快速恢复能力，保证系统数据和服务的连续性，减少对业务运营的影响。

1　备份内容

- 主机操作系统；
- 系统应用软件，如 Web 服务程序、数据库系统等；
- 运营系统软件；
- 系统上的用户化定制数据；

- 系统配置；
- 数据库用户数据。

2 备份策略

- 采用专门的备份系统对整个运营系统的软件及数据进行备份，备份数据可以保存在硬盘或其他介质上；
- 备份策略采用全备份与增量备份相结合，周一至周六进行增量备份，周日进行全备份；
- 备份策略保证没有数据丢失或数据丢失不会造成实质性的影响；
- 在系统出现故障、灾难时，备份方案能够在最短的时间内从备份数据中恢复出原系统及数据；
- 选择的备份介质能保证数据的长期可靠，并定期更新；
- 对备份数据收集、保管、押运、恢复进行管控，确保备份数据的安全，防止泄露和未经授权使用，备份数据存放在本运营站点以外安全的地方，比如灾难恢复中心；
- 定期检查备份系统和设备的可靠性和可用性，定期检查备份介质可靠性和数据完整性；
- 定期对系统数据备份进行测试检查，确保其可用性，每日对前一日产生的系统备份数据进行可用性测试，每月进行一次备份数据库可用性恢复测试检查，确保系统备份数据库可用性。

6.5.1.10 容灾备份

四川CA主机房建立了链路、网络、主机、系统、数据库冗余机制，同时在异地建立了数据容灾备份，并制定了备份恢复计划和应急响应预案。

6.5.1.11 损害和灾难恢复

1 事故和损害处理程序

四川 CA 制定了各种应急处理方案，规定了相应的事故和损害处理程序，这些应急处理方案有：

- 认证系统应急方案；
- 电力系统应急方案；
- 消防应急方案；

- 网络安全应急方案；
- 密钥应急方案等。

2 计算机资源、软件和/或数据的损坏

四川 CA 对业务系统及其他重要系统的资源、软件和/或数据进行了备份，并制定了相应的应急处理流程，当出现计算机资源、软件和/或数据的损坏时在最短的时间内恢复被损害的资源、软件和/或数据。

3 实体私钥损害处理程序

对于实体证书私钥的损害，四川 CA 有如下处理要求和程序：

- 当证书订户发现实体证书私钥损害时，订户必须立即停止使用其私钥，并立即访问四川 CA 或相应的注册机构的证书服务网站撤销其证书，或者立即通过电话、电子邮件的方式通知四川 CA 或注册机构撤销其证书。四川 CA 按 6.1.4.7 发布证书撤销信息；
- 当四川 CA 或注册机构发现证书订户的实体证书私钥受到损害时，四川 CA 或注册机构将立即撤销证书，并通知证书订户，订户必须立即停止使用其私钥。四川 CA 按 6.1.4.7 发布证书撤销信息；
- 当四川 CA 的 CA 证书或其受委托的 CA 证书出现私钥损害时，四川 CA 将立即撤销该 CA 证书并及时通过广达的途径通知依赖方，然后生成新的 CA 密钥对、签发新的 CA 证书。

4 灾难后的业务存续能力

四川 CA 建立了数据备份中心，当发生灾难事故时，能够根据业务连续性计划进行数据恢复。

5 业务连续性计划的保障方案包括：

A. 建立 CA 中心的业务可持续性计划，并进行经常检查和更新，确保其持续有效。

B. 对 CA 系统中的重要部件制订完善的灾难恢复流程，并经常进行演练，确保流程操作的有效性。

C. 建立重要系统、数据、软件的备份，并存放在符合 CPS 要求的安全环境中，确保只有合理授权人员才可接触备份。

D. 定期测试备份设备、设施、后备电源等，确保其可用性。

E. 建立当 CA 签名密钥可信性受威胁时的应变计划。

F. 制订相关流程，对 CA 中心终止服务时的告知及业务承接作出计划。

6.5.1.12 认证机构或注册机构终止

当四川 CA 及其注册机构需要停止其业务时，将会严格按照《电子政务电子认证服务管理办法》的要求，处理好相关承接事项，包括认证机构或注册机构档案记录管理者的身份问题。

- 四川 CA 拟暂停或者终止认证服务的，会在暂停或者终止认证服务六十个工作日前，选定业务承接认证机构，就业务承接有关事项作出妥善安排，并在暂停或者终止认证服务四十五个工作日前向国家密码管理局报告。
- 不能就业务承接事项作出妥善安排的，会在暂停或者终止认证服务六十个工作日前，向国家密码管理局提出安排其他认证机构承接业务的申请。

6.5.2 认证系统技术安全控制

6.5.2.1 密钥对的生成和安装

1 生成公、私钥对的实体。

包括：证书持有者、注册机构或认证机构。

2 密钥对的产生

- CA密钥对的产生

对于四川 CA 的 CA 密钥对，四川 CA 专门的密钥管理员及秘密分管者，在四川 CA 屏蔽机房中，按照四川 CA 密钥生成规程产生。四川 CA 密钥生成规程规定了 CA 密钥产生的流程控制及参加人员。四川 CA 的 CA 的密钥对使用符合国家密码主管部门的要求的密码硬件产生。

- 订户密钥对的产生

对于个人证书和机构证书，订户使用国家密码管理部门许可的密码模块（如 USB Key）生成密钥对。

对于服务器证书，订户使用服务器程序使用的密码模块（包括 SSL 硬件加速卡）提供的密钥生成功能生成密钥对。

对于运营设备证书，四川 CA 或其注册机构将使用专门的程序软件在国家密码管理部门许可的密码模块（如加密机）中生成密钥对。

对于管理员证书，私钥使用国家密码管理部门许可的客户端密码模块（如 USB Key）产生。

3　私钥传送给订户

四川 CA 各类 CA 证书密钥对由四川 CA 在其运营场地产生，私钥由四川 CA 自身持有和保存，不存在私钥的传送问题。

四川 CA 各种运营设备证书的密钥对由四川 CA 或其注册机构在设备所在地产生，并在本地保存，不存在私钥的传送问题。

对于四川 CA 签发的其他最终用户证书，通常的情况下密钥对在订户本地的密码模块（如 USB Key）中产生，私钥由最终用户保存在本地密码模块中，不存在私钥的传送问题。但在一些特殊情况下，四川 CA 或其注册机构可能会代替最终用户在用户的密码硬件中（如 USB Key）产生证书密钥对，且私钥保存在密码硬件中。在这种情形下，四川 CA 或其注册机构将通过安全的途径将保存有证书私钥的密码硬件传送到最终用户手中，并确保在传送过程中私钥不会被非授权的使用、被泄露或被损坏。

4　公钥传送给证书签发机关

需要四川 CA 认证的证书公钥，订户通过 PKCS#10 格式的证书签名请求信息文件包格式，以电子的方式将公钥提交给四川 CA 认证中心（或通过其注册机构提交），这些请求通过网络传送时使用安全套接层协议（SSL）和其他安全协议。

5　CA公钥传送给依赖方

对于四川 CA 的根 CA 公钥，通过如下方式传输给依赖方：

1）依赖方访问四川 CA 的证书服务站点下载 CA 证书，该站点受到服务器证书的保护，或，

2）依赖方访问四川 CA 的目录系统，或，

3）四川 CA、注册机构或其合作伙伴到依赖方业务系统现场将 CA 证书安装到业务系统中，或，

4）四川 CA、注册机构或其合作伙伴通过签名电子邮件将 CA 证书传输给依赖方，或，

5）四川 CA、注册机构或其合作伙伴分发给依赖方的软件中绑定、包含有 CA 证书。

对于四川 CA 的其他 CA 公钥，除了上面所述的方式传输给依赖方外，当证书订户获取证书时四川 CA 通过 PKCS#7 格式将除根证书外的证书链传递给订户。

6　密钥长度

四川 CA 的 CA 和订户密钥对至少是 256 位 SM2。

7　公钥参数的生成和质量检查

符合国家密码管理部门的要求。

8　密钥使用目的

根 CA 的密钥用于签发运营 CA 的证书及 CRL，运营 CA 的密钥用于签发订户证书。

6.5.2.2 私钥保护和密码模块工程控制

1　密码模块的标准和控制

四川 CA 使用国家密码管理部门认可、批准的加密机生成根 CA、证书签发 CA 和其他 CA 密钥对，并存储 CA 私钥。

四川 CA 制定有专门密码管理策略，在从运送、验收、初始化、存储、使用到销毁的整个密码设备生命周期内，对密码模块进行管理和控制。CA 密码模块离线存放在 CA 密钥离线存放区中，CA 密码模块在线放置在屏蔽机房或机柜中。

四川 CA 运营设备证书使用的密码模块的标准及控制同 CA 密钥密码模块。

最终用户证书使用国家密码管理部门认可的密码模块，并妥善保护、保管其密码模块，防止其失窃、丢失、损坏及被非授权的使用。

2　私钥多人控制

四川 CA 的 CA 私钥存放在加密机中，加密机管理员 IC 卡设置 3 张，采用 3 选 2（3 of 2）多人控制策略控制加密机管理员权限的激活、使用，只有当管理员权限激活后，才能进行密钥生成、密钥备份、密钥恢复、密钥销毁。

加密机数据备份 IC 卡设置 5 张，密钥备份时采用 5 张 IC 卡存放数据备份秘密分割，密钥恢复时采用 5 选 3（5 of 3）多人控制策略控制密钥恢复。

3　私钥托管

四川 CA 所有 CA（包括根 CA 和运营 CA）的私钥均未在其他地方托管。

四川 CA 根据国家密码管理部门的要求对订户加密证书的私钥进行托管。

4　私钥备份

四川 CA 对 CA 私钥通过专门的备份加密机进行备份，这些备份分别作为本地常规备份。

对于认证机构运营设备证书，四川 CA 或其注册机构通常不进行私钥备份；但对某些特别的运营设备证书，如时间戳服务证书，四川 CA 会对其私钥进行备份。

对于最终用户证书，如果存放证书私钥的密码模块允许私钥备份，四川 CA 建议订户对私钥进行备份，并对备份的私钥采用口令或其他访问控制机制保护，防止非授权的修改或泄露。

5　私钥归档

当四川 CA 的 CA 密钥对超过使用期后，这些 CA 密钥对将归档保存至少十年。归档 CA 密钥对保存在本节第 1 条所述的加密机中，并且四川 CA 的密钥管理策略和流程阻止归档 CA 密钥对返回到产品系统中。对归档私钥到了归档保存期，四川 CA 将按本节第 10 条销毁。

对于认证机构运营设备证书，四川 CA 或其注册机构通常不进行私钥归档，因为这种归档是不需要的；但对某些特别的运营设备证书，如时间戳证书，四川 CA 会对其私钥进行归档，其归档过程和要求同 CA 密钥对。

四川 CA 或其注册机构不对最终用户证书的私钥进行归档，但如果订户存放证书私钥的密码模块允许私钥备份，四川 CA 建议订户对私钥进行归档，并对归档的私钥采用口令或其它访问控制机制保护，防止非授权的泄露。

6　私钥导入、导出密码模块

四川 CA 的 CA 密钥对在加密机上生成，保存和使用。此外，为了常规恢复和灾难恢复，四川 CA 对 CA 密钥进行复制。当 CA 密钥对从一个加密机复制到另一个加密机上时，被复制的密钥对以加密的形式在模块之间传送，并且在传递前要进行模块间的相互身份鉴别。另外四川 CA 还有严格的密钥管理流程对 CA 密钥对复制进行控制。所有这些有效防止了 CA 私钥的丢失、失窃、修改、非授权的泄露、非授权的使用等。

四川 CA 运营设备证书私钥的导入、导出控制同 CA 私钥。

四川 CA 注册机构的运营设备证书私钥通常是不允许导入、导出的，若在特定的情况下确实需要导出、导入，则必须由四川 CA 的可信人员进行相关的操作。四川 CA 在进行导出、导入时，将确保导出的证书私钥不以明文形式存在（如由具有足够强度的口令保护），并在完成导出、导入后立即、彻底地销毁导出的私钥。

对于各类最终用户证书，若使用的密码模块（软件或硬件）支持私钥的导出、导入，则四川 CA 要求最终对导出、导入的私钥必须使用足够安全的口令进行保护，且最终用户需要确保导出的私钥不被丢失、失窃、修改、非授权的泄露、非授权的使用等。

7　私钥在密码模块的存储

四川 CA 的 CA 私钥以加密的形式存放在符合国家密码主管部门的要求加密机中，且私钥的使用也在加密机中进行。

四川 CA 运营设备证书私钥的存储同 CA 私钥。

对于个人证书和机构证书，最终用户须将私钥保存在其可控制、国家密码主管部门的

认可的密码模块中（如 USB Key），私钥在密码模块中须以加密形式存储，且私钥的使用受口令或指纹等安全措施保护。最终用户须采取必要的措施防止其他人员对私钥的非授权访问、获取和使用。

对于服务器证书，最终用户需将私钥保存在国家密码主管部门认可的密码模块中（包括 SSL 加速卡），且存放私钥的密码模块必须在最终用户其可控制的范围内，并最终用户要采取相应的安全手段防止对私钥的非授权访问、获取和使用，使用的手段包括私钥的使用受口令保护，服务器及密码模块位于安全可控的物理环境等。

8 激活私钥的方法

- 最终用户证书私钥

保存在密码模块中的最终用户证书私钥需在用户输入口令（或 PIN 码）或指纹等密钥保护信息（激活数据）后才被激活，才能能够被使用。

- 运营设备证书私钥

对于四川 CA 的运营设备证书私钥的激活同 CA 私钥的激活；对于四川 CA 注册机构的运营设备证书私钥，需要专门的安全管理人员输入保护口令后才能激活。

- CA 私钥

四川 CA 的 CA 私钥存放在加密机中，并且其激活数据按本节第 2 条进行分割。当需要使用 CA 私钥时（在线或离线），需要召集齐最小门限值的秘密共享持有者才能激活。

9 解除私钥激活状态的方法

对于个人证书和机构证书，当应用软件向密码模块发出设备关闭指令，或密码模块被下载（如硬件密码模块从读卡器中取出）、或用户通过密码管理软件从密码设备登出（logout）、或计算机断电时，私钥被解除激活状态，不能再被使用。

对于服务器证书，当服务程序关闭、系统注销或系统断电后私钥即进入非激活状态。

对于四川 CA 或其注册机构的运营设备证书的私钥，当 CA 或 RA 系统向密码模块发出登出（logout）或密码管理软件向密码模块发出关闭（close）指令，或存放私钥的密码模块断电,，私钥进入非激活状态。

对于四川 CA 的 CA 私钥，当 CA 系统向密码模块发出登出（logout）或密码管理软件向密码模块发出关闭（close）指令，或存放私钥的加密机断电,，私钥进入非激活状态。

10 销毁私钥的方法

对于四川 CA 的最终用户证书私钥，若不再使用，将私钥销毁，从而避免丢失、偷窃、

泄露或非授权使用。若私钥撤销、到期作废后，还需要用于信息解密的，最终用户应该妥善保存一定期限，以便于解开加密信息。若私钥无需再保存，则将通过私钥的删除、系统或密码模块的初始化来销毁。

在四川 CA 的 CA 私钥生命周期结束后，四川 CA 将 CA 私钥继续保存在一个备份加密机中，并进行归档，其他的 CA 私钥备份被安全销毁。归档的 CA 私钥在其归档期限结束后，需在多名可信人员参与的情况下安全销毁。CA 私钥的销毁将确保 CA 私钥从加密机中彻底删除，不留有任何残余信息。

四川 CA 不再使用的运营设备证书私钥，按 CA 私钥销毁相同的方法进行销毁，对无需归档而不再使用的运营设备私钥将立即销毁。

四川 CA 注册机构不再使用的运营设备证书私钥，将通过私钥的删除、系统或密码模块的初始化来销毁。

11 密码模块的评估

由国家密码管理部门负责。

6.5.2.3 密钥对管理的其他方面

1 公钥归档

对于生命周期外的 CA 和最终用户证书，四川 CA 将进行归档，归档的证书存放在归档数据库中。

2 证书操作期和密钥对使用期限

四川 CA 会在用户申请审核鉴定通过，用户并付款后 5 个工作日内将证书颁发给用户，密钥对的使用期限与证书有效期相一致，一般为 1 年。

对于 CA 证书，密钥对通过证书更新允许的最长使用期限如下：

- 对于 256 位 SM2 根 CA 证书，其密钥对的最长允许使用年限是 30 年；
- 对于 256 位 SM2 中级 CA 证书，其密钥对的最长允许使用年限是 20 年。

A. 公钥和私钥的使用期限与证书的有效期相关但却有所不同。

B. 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数字签名，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。

C. 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。

D. 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。

E. 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。

6.5.2.4 激活数据

1 激活数据的产生和安装

四川 CA 的 CA 私钥的激活数据由加密机内部产生，并分割保存 IC 卡中，需通过专门的读卡设备和软件读取。四川 CA 的 CA 私钥激活数据的产生过程，按四川 CA 密钥生成规程进行。所有秘密共享的创建和分发有相应的记录，包括产生时间、持有人等信息。

四川 CA 运营设备证书私钥的激活数据的产生和安装，同 CA 私钥。

四川 CA 注册机构运营设备证书私钥的激活数据，由注册机构的安全管理员根据所用密码系统提供的功能相应产生。若激活数据是口令，则对口令的安全要求不低于订户证书私钥保护口令的要求。

如果订户证书私钥的激活数据是口令，这些口令必须：

- 由用户产生；
- 至少 8 位字符或数字；
- 至少包含一个字符和一个数字；
- 至少包含一个小写字母；
- 不能包含很多相同的字符；
- 不能和操作员的名字相同；
- 不能包含用户名信息中的较长的子字符串。

四川 CA 还建议订户使用双因素机制（如硬件+密码，生物识别设备+密码等）来控制私钥的激活。

2 激活数据的保护

保存有四川 CA 的 CA 私钥及运营设备证书私钥的激活数据秘密分割的若干张 IC 卡，由四川 CA 若干个不同的可信人员持有，而且持有人员必须符合职责分割的要求，签署协议确认他们知悉秘密共享者责任。秘密共享由持有人分别存放在四川 CA 保险柜中。

四川 CA 注册机构的运营设备证书私钥的激活数据，由注册机构的管理员负责安全保护。

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。

3　激活数据的其他方面

1）激活数据的传送

存有四川 CACA 私钥、运营设备证书私钥的激活数据的 IC 卡，通常保存在四川 CA 的安全设施中，不能携带外出或传送。如因某种特殊情况确实需要传送时，其传送过程需在四川 CA 安全管理人员和密钥管理人员的监督下进行。

四川 CA 注册机构的运营设备证书私钥的激活数据由注册机构的安全管理员产生、保管，不得向外传送。

通常情况下订户证书私钥的激活数据由订户自己产生、保管，不应传送给其他人员，若私钥激活数据因特别的原因需要进行传送时，订户应保护它们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

在某些特别的安排下，四川 CA 认证中心或其注册机构，有可能代订户在特定的密码硬件（如 USB Key）中产生私钥并产生相应的激活数据，在这种情况下，四川 CA 或其注册机构，或者通过面对面的方式，或者通过电话、电子邮件等方式，将激活数据传送给订户。在非面对面的传送方式下，私钥激活数据的传送路径、方式同存有私钥的密码硬件的传送路径、方式将是不同的，分开的。在这种安排下，订户在接收到存有私钥的密码硬件和获得激活数据后，必须尽快改变私钥的激活数据。

2）激活数据的销毁

存有四川 CACA 私钥、运营设备证书私钥的激活数据分割的 IC 卡，其销毁所采取的方法包括将 IC 卡初始化，或者彻底销毁 IC 卡，无论采取何种方式，都将保证不会残留有任何秘密信息。CA 私钥激活数据的销毁是在四川 CA 安全管理人员和密钥管理人员的监督下进行。

四川 CA 注册机构的运营设备证书私钥的激活数据不再使用时，注册机构掌管激活数据的安全管理员需要销毁有关数据，确保无法通过残余信息、介质直接或间接恢复激活数据的部分或全部。

当订户证书私钥的激活数据不需要时应该销毁，订户应该确保无法通过残余信息、介质直接或间接恢复激活数据的部分或全部，比如记录有口令的纸页必须粉碎。

6.5.2.5 系统安全控制

1　特别的系统安全技术要求

四川 CA 的证书认证系统主机实现了自主访问控制（DAC），进行了安全漏洞扫描和安全优化，安装了防病毒系统，确保了包含 CA 软件和数据文件的系统是安全可信的系统，不会受到未经授权的访问。此外，根据四川 CA 的安全策略，只允许有工作需求的必要人员访问生产系统的服务器，一般的应用用户在生产系统服务器上没有账户。

四川 CA 的电子认证生产系统网络与其它部分逻辑分离，并使用防火墙阻止从内网和外网入侵生产系统网络，限制访问生产系统的活动，且只有四川 CA 系统运营管理组中的、必要的可信人员可以直接访问认证系统数据库。

系统口令必须符合口令安全管理要求。

2　系统安全评估

四川 CA 的 CA 系统及其运营环境通过了国家权威机构的安全测评、评审，并获得了相应资质。

6.5.2.6 生命周期安全控制

1. CA 系统运行管理

A. CA 系统的操作流程采用文档化并进行维护。

B. CA 系统（包括软件、网络等方面）的变更按系统变更控制流程经管理层批准，经批准的变更实行前通过测试验证，并进行记录。

C. 可能对系统的安全性有影响的改动必须事先由管理层得进行风险评估，改动前进行备份并得到管理层的明确批准。

D. CA 中心的测试系统、运营系统、网络设施等，都由专门的操作维护人员，并有相应明确的授权。

E. 操作维护人员定期检查系统及网络的稳定性、安全性及容量，确定符合服务水平。

F. 建立了检测和防护控制来防止病毒和恶意软件，并能提供适当的报警信息。

G. 建立了监控流程，确保记录并报告发现的或怀疑的、对系统或服务有威胁的安全缺陷。建立并执行系统故障报告、处理流程。

H. 建立了相应制度，对 CA 系统相关的媒介（包括设备、证书介质、文档等）进行妥善保管，避免非授权的访问。

2. CA 系统的访问管理

A. 制定了 CA 系统的访问策略，内容包括：访问角色及相关权限，认证及鉴别的方法，

分权机制，特殊 CA 操作的人数（密钥生成时 3/2 规则）等。

B. 制定了 CA 系统访问人员角色职能定义，确保合理的职责分割和权限控制，并明确授权及取消授权的操作流程和策略。

C. 制定了网络安全策略，并制定了访问网络的控制策略。

D. 制定了操作系统及 CA 软件的安全访问的策略。

E. 建立了对各种对 CA 系统访问的审计措施。

3. CA 系统的开发和维护

A. 建立了 CA 系统软件修订控制流程，对系统新增或修改进行管理。

B. 严格控制对 CA 系统的源代码及测试数据的访问。

C. 操作系统升级变更时，对应用系统软件重新测试。

D. 在 CA 系统中，购买、使用或修改的软件，严格检查，避免“特洛伊木马”等攻击。

6.5.2.7 网络安全控制

四川CA证书认证系统的网络环境部署了防火墙、入侵检测、防病毒、安全身份认证等安全技术，确保认证系统的安全运营，对于认证系统的网络安全制定了专门的网络安全策略与应急响应方案，定期巡检、定期升级安全措施（包括入侵检测、漏洞扫描、打补丁等），避免网络攻击和漏洞等带来运营风险。

CA系统运行、网络安全和安全审计等措施符合GM/T 0034的要求。

6.5.2.8 时间戳

四川CA部署有时间戳系统，在系统关键业务运行日志、操作日志等日志中，都有可靠的记录时间，使用了可靠的时间源及时间戳服务。

四川CA签发的数字证书、CRL、OCSP响应以及时间戳服务响应包含有时间及日期信息，且这些时间和日期信息是经过数字签名的。

7 电子政务电子认证服务中的法律责任相关要求

7.1 要求

四川CA在开展电子认证服务时，严格按照《电子签名法》、《电子政务电子认证服务管理办法》等法律法规的要求，对涉及保密、隐私、知识产权、担保以及服务运营等各方面承担相关的责任与义务。

四川CA与证书用户签署证书服务协议，明确双方法律责任与义务，以及安全保管要求。通过授权的机构或代理机构提供电子认证服务时，由授权的机构或代理机构与证书用户签署证书服务协议，明确相关法律责任与义务。

四川CA在本CPS中明确一般性的业务和法律问题。在业务条款中说明不同服务的费用问题，和各参与方为了保证资源维持运营，针对参与方的诉讼和审判提供支付所需承担的财务责任；法律责任条款涉及保密、隐私、知识产权、担保及免责等内容，具体涵盖的内容见“7.2内容”。

7.2 内容

7.2.1 费用

1 证书服务涉及的费用标准：

- 四川 CA 根据市场与证书实际应用的需要确定证书价格。在订户订购证书时，将提前告知证书的签发与更新费用；
- 四川 CA 不收取证书查询费用；
- 免费提供证书撤消和撤消列表（CRL）查询；
- 四川 CA 有可能根据需要将在线查询（OCSP）服务作为增值服务收取费用。

2 退款规定

在实施证书操作和签发证书的过程中，四川 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，四川 CA 将不办理退证、退款手续。

如果由于四川 CA 的原因，造成订户合同无法履行、订户证书无法使用，四川 CA 将费用返还给订户。

如果由于不可抗力因素导致四川 CA 暂停、终止部分或全部电子签名认证证书服务，四川 CA 不承担退款责任。

7.2.2 财务责任

1 保险范围

四川 CA 向证书订户提供证书使用保障。如果由于四川 CA 原因造成用户使用证书过程中遭受损失，四川 CA 公司将向证书订户、依赖方提供赔偿（具体情形参见 7.2.9）。

2 其他资产

四川 CA 具备国家密码主管部门所规定的资金实力，具备承担赔偿责任的条件。

3 对最终实体的保险或担保

四川 CA 用户保障计划提供的服务保障针对的最终实体主要是证书订户和证书依赖方。

7.2.3 业务信息保密

四川 CA 有专门的信息保密制度，保护自身和用户的敏感信息、商业秘密。

1. 保密信息范围

四川 CA 保密的信息包括但不限于：

- 系统方面
  - 认证系统结构、配置，包括系统、网络、数据库等；
  - 认证系统安全策略和方案；
  - 系统操作、维护记录；
  - 各类系统操作口令。
- 运营管理方面
  - 物理安全策略与实施方案，包括场地、访问控制、入侵检测等实施方案；
  - 密钥管理策略与操作记录；
  - CA 或 RA 批准或拒绝的申请纪录；
  - 可信人员名单；
  - 内部安全管理策略与制度。
- 用户信息
  - 用户的注册信息；
  - 用户系统、应用访问 CRL、OCSP 的记录（时间、频度）；
  - 用户与四川 CA、注册机构签订的协议；

2. 不属于保密的信息

证书、证书状态信息及信息库中的信息，都是不需保密的信息。

3. 保护保密信息的责任

四川 CA 制定了严格的管理制定、流程和技术手段保护自身的商业秘密，并且把保护用户信息作为自己应尽的义务。四川 CA 的每个员工都要接受信息保密培训。

7.2.4 个人隐私保密

1. 隐私保密方案

四川 CA 有用户隐私计划保护证书订户的个人信息。

2. 作为隐私处理的信息

作为隐私处理的信息包括，订户注册证书中提交的、但不在证书中显示的信息，包括联系电话、地址等；个人与四川 CA、四川 CA 注册机构签订的协议。

3. 不被视为隐私的信息

不被认为是隐私信息包括，要出现在证书中的信息、证书及证书状态信息。

4. 保护隐私的责任

除非执法、司法方面的强制需要，四川 CA 及其注册机构在没有获得用户授权的情况下，不会将用户隐私信息透露给第三方。

5. 使用隐私信息的告知与同意

四川 CA 及其注册机构如果需要将用户隐私信息用于双方约定的用途以外的目的，则需要事先告知用户并获得用户同意和授权，用户同意和授权信息以下列方式之一传送给四川 CA 或其注册机构：

1）有手写签名的同意和授权文件，并将文件邮寄、快递到四川 CA 或其注册机构；

2）将手写签名的同意和授权文件传真到四川 CA；

3）以电子签名的形式同意并授权；

4）以其他可靠的形式同意并授权。

6. 依法律或行政程序的信息披露

由于法律执行、法律授权的行政执行的需要，四川 CA 或其注册机构有可能需要将有关信息在用户知晓或不知晓的情况下提供有关执法机关、行政执行机关，即使出现这种情形，四川 CA 及其注册机构也将尽可能地保护用户隐私信息。

7. 其他信息披露情形

对其他信息的披露受制于法律、订户协议。

7.2.5 知识产权

1. 证书和撤销信息中的知识产权

四川 CA 对它签发的证书、证书撤销列表及其中信息的拥有知识产权，证书公钥是订户的知识产权。

2. CPS中的知识产权

四川 CA 对本 CPS 拥有知识产权。

3. 命名中的知识产权

证书订户对证书注册信息及签发给他的证书中包含的商标、服务标志或商品名和甄别

名拥有知识产权。

4. 密钥和密钥材料的知识产权

证书中的密钥对是证书中主体对应实体或实体拥有者的知识产权。

7.2.6 陈述和担保

1. CA 的陈述与担保

订户同意四川CA订户协议是订户注册申请四川CA证书的一个条件，在订户成功完全证书申请注册前，订户必须以下列两种方式之一接受订户协议：

- 对订户协议文件签名并提交给四川CA或其注册机构；或者，
- 阅读注册页面上订户协议，并点击同意订户协议。

依赖方决定信赖四川CA签发的证书前需阅读四川CA依赖方协议，用户接受证书及状态信息即表明其接受了依赖方协议。

四川 CA 不负责评估证书是否被恰当使用。订户和依赖方必须依订户协议和依赖方协议确保证书用于允许使的目的。

四川CA、注册机构和订户之间的担保、免责和有限责任由他们之间的协议规定约束。

四川CA对证书订户做出如下担保：

- 证书中不存在批准证书申请或签发证书时四川 CA 已知的对事实的实质性错误描述；
- 批准证书申请或签发证书时，不会因为工作疏忽将错误信息包含到了证书中；
- 证书满足四川CA所有实质性的要求；
- 撤销服务和信息库的使用在所有方面符合四川CA的要求。

四川CA对证书依赖方做出如下担保：

- 除了未经鉴别、验证的订户信息外，包含在证书中的所有信息都是准确的；
- 在四川CA信息库中发布的证书已经签发给了个人或组织机构（它们的名字包含在证书中），订户已经接收了该证书；
- 批准证书申请或签发证书的实体签发证书时完全遵守了CPS的规定；
- 四川CA所采纳的与证书服务有关的技术，基于目前的技术发展与评估是安全的、可靠的；
- 四川CA已通过技术的、物理的防护及流程控制，确保服务系统、设备和设施的安全、可靠。

2. RA 的陈述与担保

四川 CA 的注册机构做出如下担保：

RA 在批准证书前，完成了所有必要的鉴证工作，并且确认了信息是正确的、准确的。

3. 订户的陈述与担保

作为获得证书的一个条件，证书申请者在证书申请时已阅读了订户协议并且同意订户协议，并且：

- 在证书申请时，订户的所有陈述都是对的；
- 订户提供的，特别是包含在证书中的需要鉴别、验证的信息是真实的、准确的。

在证书的保存和使用过程中，订户同意做到：

- 按照四川 CA 的 CPS 将证书用于规定的使用目的，不将证书用于证书使用目的以外的场合；
- 利用与证书中的公钥相对应的私钥产生的数字签名是订户的数字签名，订户知晓要签名的内容，产生数字签名时，订户已经接受了证书，且该证书没有过期或撤销；
- 订户对自己的私钥进行了有效的保护，其他人员无法使用订户的私钥。

4. 依赖方的陈述与担保

依赖方必须熟悉本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，阅读了依赖方协议，并评估了在特定应用中信赖证书的适当性，不在证书适用目的以外的应用中信任证书；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业务规则的有关条款。

5. 其他参与者的陈述与担保

为四川 CA 提供用户身份验证服务的第三方已向四川 CA 做出如下承诺，

- 是合法的、获得授权的组织机构信息服务提供商；
- 提供的信息权威性的；
- 在其能够管理与控制范围内，其提供的数据是真实的、准确的；
- 其保存的组织机构信息在最短的时间内获得了更新。

7.2.7 担保免责

四川 CA 不对其签发的证书适用于其规定的目的以外的任何应用承担任何担保，对证书在其规定的目的以外的应用不承担任何责任。对由不可抗力，如战争、地震、洪灾、爆炸、恐怖活动等，造成的服务中断并由此造成的用户损失，四川 CA 及注册机构不承担责任。

7.2.8 偿付责任限制

对于由于四川 CA 自身原因，如没有严格按业务流程进行证书审批导致证书的错误签发、假冒，或管理上的疏忽导致 CA 私钥泄漏、盗用等，造成了证书订户、依赖方的损失，四川 CA 将承担相应的赔偿责任，但这种责任是有限的。

四川 CA 对于证书提供的保障级别分为：恢复证书使用、撤销（错误）证书、经济赔偿。

对于设备证书不涉及经济赔偿，只涉及恢复证书使用、撤销（错误）证书等方式的保障。对于个人证书和机构证书，在包括上述保障方式外，增加经济补偿保障方式，见下表。

证书级别	*责任赔偿*
个人证书	最高人民币 800 元
机构证书	最高人民币 4,000 元

四川 CA 只对由于自身原因造成的用户直接损失承担责任，对间接的损失不承担责任。

7.2.9 赔付责任

有下列情形之一的，四川 CA 承担有限的赔偿责任：

- 四川 CA 将证书错误的签发给订户以外的第三方，导致订户或者依赖方遭受损失的；
- 订户提交的注册信息或者资料真实、完整、准确，但四川 CA 签发了有错误信息的证书，导致订户或者依赖方遭受损失的；
- 由于四川 CA 的原因导致证书私钥被破译、窃取，致使订户或者依赖方遭受损失的。

订户有下列情形之一，给四川 CA、依赖方造成损失的，应当承担赔偿责任：

- 提供的资料或者信息不真实、不完整或者不准确的；
- 证书中的信息有变更，未终止使用该证书并通知各方的；

- 订户没有使用可信系统保护私钥，或者没有采取必要的注意防止订户私钥的安全损害、丢失、泄漏、修改或非授权的使用；
- 知悉证书私钥已经丢失或者可能已经丢失时，未终止使用该证书并通知各方的；
- 订户使用的名字（包括但不限于通用名、域名和 e-mail 地址）破坏了第三方的知识产权的；
- 超过证书的有效期限使用证书的；
- 使用证书用于违法、犯罪活动的。

在如下情况，依赖方对自身原因造成的四川 CA 损失承担责任，

- 依赖方没有执行依赖方职责义务；
- 依赖方在不合理的环境下信赖一个证书；
- 而依赖方没有检查证书状态确定证书是否过期或撤销。

有下列情形之一的，四川 CA 不承担赔付责任：

- 因订户原因致使依赖方遭受损失的；
- 依赖方未经检验证书的状态即决定信赖证书的；
- 依赖方明知或者应当知道证书存在超范围使用、超期限使用、被人窃取或者信息错误等情况，仍然信赖该证书并从事有关活动的；
- 因不可抗力原因导致订户或者依赖方遭受损失的。

7.2.10 有效期和终止

1. 有效期限

除非四川 CA 特别声明 CPS 提前终止，在四川 CA 颁布新版本的 CPS 之前，本 CPS 一直有效。

2. 终止

当四川 CA 终止业务时，四川 CA 的 CPS 终止。

3. 效力的终止与保留

四川 CA 的 CPS 的终止（而非更新），意味着四川 CA 认证业务的终止。四川 CA 终止认证业务的过程将按国家有关主管部门的规定进行，并根据规定对受影响的用户进行安排，保证用户的利益不受影响或将受影响的程度减少到最小。

当由于某种原因，如内容修改、与适用法律相冲突， CPS、订户协议、依赖方协议和其他协议中的某些条款失效后，不影响文件中其他条款的法律效力。

7.2.11 对参与者的个别通告与沟通

四川 CA 或其注册机构在必要的情况下，如在主动撤销订户证书、发现订户将证书用于规定外用途及订户其他违反订户协议的行为时，会通过适当方式，如电话、电邮、信函、传真等，个别通知订户或订户所属机构、依赖方。

7.2.12 修订

1. 修订程序

本认证业务规则将尽量避免不必要的修改。但不定期地，四川 CA 将对本 CPS 进行检查、评估，当四川 CA 认为应该对本 CPS 做出修改时，四川 CA CPS 编写小组将对本 CPS 及其他相关文档、协议提出修改建议，获得四川 CA 安全策略委员会批准后正式发布。

2. 通知机制与期限

四川 CA 将修改了的 CPS 通过四川 CA 信息库更新通告栏发布。在认为有必要时，四川 CA 将通过电子邮件、信件、媒体等方式通知有关各方。

修改后的 CPS 经批准后将立即在四川 CA 信息库更新通告栏发布。对于需要通过电子邮件、信件、媒体等方式通知的修改，四川 CA 将在合理的时间内通知有关各方，合理的时间保证有关方面受到的影响最小。

3. 必须修改业务规则的情形

由四川 CA 安全策略委员会根据公司业务情况决定。

7.2.13 争议处理

当四川 CA、订户和依赖方之间出现争议时，有关方面可依据协议通过协商解决，协商解决不了的，可通过法律解决。

争议处理流程为：

1. 争议解决的通知

当争议发生时，在采取任何行动措施之前，订户或依赖方应首先通知四川 CA。

2. 争议解决的方式

如果争议在最初通知之日起 10 个工作日内未被解决，四川 CA 将召集由 3 名安全认证专家组成外部专家小组。外部专家小组以协助解决争议为目的，收集相关事实。专家小组在成立之日起 10 个工作日内（除非当事人同意将此段时限延长至一特定时段）完成建议并向当事人传达。专家小组的建议对当事人无约束力，但当事人一方若书面签署文件表示同意该建议，则争议的双方即按照建议的内容解决争议。如果订户或依赖方在书面签署

文件同意专家小组建议后后悔，并将争议提交法院，则该建议将视为 四川 CA 与订户或依赖方之间就争议解决达成的协议且受法律保护。

3. 正式争议解决

若专家小组未能在约定时限内提出有效建议，或者所提的建议不能使双方当事人就争议的解决达成一致意见，争议双方可以将争议提交四川 CA 所在地有管辖权的法院。

4. 索赔时限

任何订户或依赖方欲向四川 CA 提出索赔，应在知道或应当知道损失发生时起的两年内提出。超出两年的，该索赔无效。

7.2.14 管辖法律

对本 CPS 生效和解释起作用的有关法律、法规，主要有：

- 《中华人民共和国电子签名法》;
- 《电子政务电子认证服务管理办法》。

7.2.15 与适用法律的符合性

四川 CA 电子认证服务活动参与者所需遵守的适用法律， 如与密码硬件和系统相关的法律， 服务监管的法律，主要有：

- 中华人民共和国电子签名法
- 中华人民共和国网络安全法
- 商用密码管理条例
- 电子认证服务密码管理办法
- 电子政务电子认证服务管理办法

7.2.16 一般条款

1. 完整协议

CPS、订户协议及依赖方协议及其补充协议将构成四川 CA 与订户、依赖方之间的完整协议。

2. 转让

四川 CA、注册机构、订户及依赖方之间的责任、义务不能通过任何形式转让给其他方。

3. 分割性

法律允许的范围内，在四川 CA 订户协议、依赖方协议和其他订户协议内出现可以同其他条款分割的条款时，协议中的可分割条款的无效不影响协议中其他条款效力。

4. 强制执行

在四川 CA、注册机构、订户和依赖方之间出现纠纷、诉讼时，胜诉可以要求对方支付有关诉讼费作为对其补偿的一部分。免除一方对某次合同违约的赔偿不意味着免除对其他合同违约的赔偿。

5. 不可抗力

当由于不可抗力，如地震、洪灾、雷电等自然灾害和战争等，造成四川 CA、注册机构无法提供正常的服务时，四川 CA、注册机构不承担由此给用户造成的损失。

7.2.17 其他条款

四川 CA 对本《电子政务电子认证业务规则》拥有最终解释权。