四川省数字证书认证管理中心有限公司

国密 SSL 证书电子认证业务规则

V1.0 版

发布日期：2022 年 9 月 1 日

生效日期：2022 年 9 月 1 日

@SCCA 四川省数字证书认证管理中心
SICHUAN DIGITAL CERTIFICATE AUTHORITY MANAGEMENT CENTER

版权声明

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

邮编：610041

电话：+86-28-85336171

传真：+86-28-85336171-808

版本控制表：

版本	主要修改说明	审核/批准人	生效时间
1.0	根据 CA/B Forum 上 Baseline Requirements 的要求，按照 RFC3647 框架编写，形成版本。	四川CA安全策略委员会	2022年9月1日

目　录

1. 概括性描述

1.1 概述

1.1.1 公司简介

四川省数字证书认证管理中心有限公司（简称四川CA），成立于2007年11月，是具有工信部颁发的《电子认证服务许可证》和国家密码管理局颁发的《电子认证服务使用密码许可证》的权威、公证、第三方电子认证服务机构。四川 CA 秉承“共建可信网络、赋能数字生态”的发展理念，基于国产商用密码，依据我国《电子签名法》、《网络安全法》、《密码法》，面向政府、企业、个人提供各类数字证书的签发、更新、吊销等管理服务，通过以PKI技术、数字证书应用技术为核心的产品和服务，为网上业务活动提供可信身份、可信行为、可信时间、可信结果的网络信任环境，解决用户身份真实、数据完整、行为不可抵赖等安全问题。

1.1.2 电子认证业务规则（CPS）

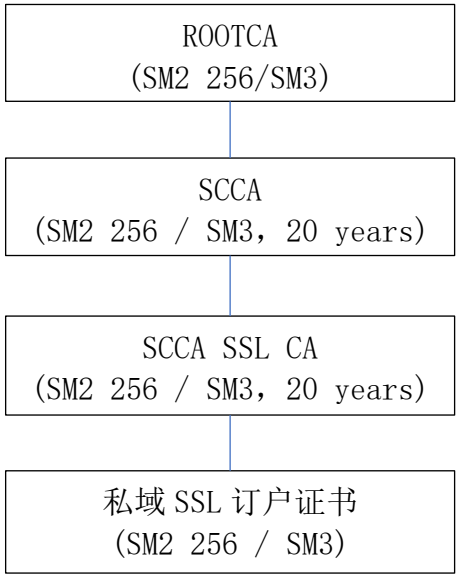
本《国密 SSL 证书电子认证业务规则》（简称本 CPS）的总体条款结构符合工业和信息化部所发布的《电子认证业务规则规范（试行）》，并在制定过程中遵循《中华人民共和国电子签名法》、《电子认证服务管理办法》、以及《电子认证服务密码管理办法》等法律法规的要求，本 CPS 同时遵循 RFC3647 的框架进行编写，阐明了四川CA如何开展电子认证业务，包括批准、签发、管理、吊销和更新SSL证书的业务方式和过程，以及相应的服务、法律和技术上的措施和保障，以供电子认证活动参与方了解和遵循，各参与方必须完整地理解和执行本CPS所规定的条款，并承担相应的责任和义务。

本 CPS 所阐述的内容遵循四川CA证书策略，适用于国家密码管理局认可的密码算法所签发的数字证书，四川CA参照CA/Browser论坛对证书的签发和管理要求进行签发证书，并遵循 WebTrust 国际审计标准进行运营管理。四川CA定期跟踪国内外法律法规、标准和政策的变化及更新情况，并将持续根据其变化、更新进行修订本CPS。

1.1.3 证书体系架构

本 CPS 中的国密 SSL 证书信任体系有 2 个根证书，分别是 ROOTCA 证书、SCCA Root CA1 证书，其中 ROOTCA 证书是国家密码管理局根证书，SCCA Root CA1 证书是四川 CA 的根证书，每个根证书下设中级 CA 签发订户证书，四川 CA 不签发外部中级 CA 证书。

1）ROOTCA



ROOTCA 证书是国家密码管理局的根证书，密码算法为 SM2，密钥长度为 256-bit；SCCA 是 ROOTCA 签发的运营 CA 二级根证书，密码算法为 SM2，密钥长度为 256-bit；SCCA 下设 SCCA SSL CA 证书，密码算法为 SM2，密钥长度为 256-bit，用于签发密钥长度为 SM2 256-bit 的私域 SSL 服务器证书。

根 CA 证书信息如下：

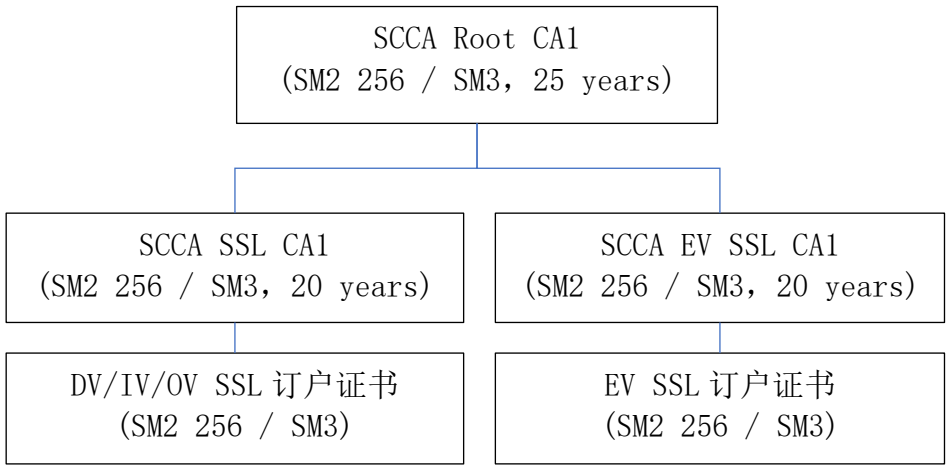
根名称	SCCA（国家电子认证根 CA 签发的二级根）
国家	CN
组织	Sichuan Digital Certificate Authority Management Center
通用名	SCCA
颁发者	ROOTCA（国家电子认证根 CA 的社会公众应用根证书 SM2）
颁发机构密钥标识符	4C32B197D9331BC4A605C1C6E58B625BF0977658
主题密钥标识符	C08DDE970FF0020B3EFF741A534764DC69D5A71F
序列号	3C4AF5224F0F36A491AEB7313030F9AC
有效期	20 年

起始日期	2016年4月22日 15:15:31
到期日期	2036年4月17日 15:15:31
算法	SM2(256 bits)
签名算法	SM3withSM2

中级CA证书信息如下：

中级CA名称	SCCA SSL CA
国家	CN
组织	Sichuan Digital Certificate Authority Management Center
通用名	SCCA SSL CA
颁发者	SCCA
颁发机构密钥标识符	C08DDE970FF0020B3EFF741A534764DC69D5A71F
主题密钥标识符	6FC80294E286BCD97AD2E0952FF5C88A506ECC92
序列号	64AA027B9B43009B63E2A6B24B8FCD0D688387B5
有效期	20年
起始日期	2016年5月18日 15:29:41
到期日期	2036年5月13日 15:29:41
算法	SM2(256 bits)
签名算法	SM3withSM2

2）SCCA Root CA1



SCCA Root CA1证书的密码算法为SM2，密钥长度为256-bit，下设2个中级CA证书，其中：（1）SCCA EV SSL CA1，密钥长度为256-bit，用于签发密钥长度为SM2 256-bit

的EV SSL服务器证书；（2）SCCA SSL CA1，密钥长度为256-bit，用于签发密钥长度为SM2 256-bit的DV/IV/OV SSL服务器证书。

根CA证书信息如下：

根名称	SCCA Root CA1
国家	CN
组织	Sichuan Digital Certificate Authority Management Center
通用名	SCCA Root CA1
颁发者	SCCA Root CA1
颁发机构密钥标识符	2317FE4C18A9B21E30EE057EB228F9D4603CECAD
主题密钥标识符	2317FE4C18A9B21E30EE057EB228F9D4603CECAD
序列号	4C72B7D1107CA83C3E21D4B470D67433E3BF51C4
有效期	25 年
起始日期	2022年8月29日 14:57:37
到期日期	2047年8月29日 14:57:37
算法	SM2(256 bits)
签名算法	SM3withSM2

中级CA证书信息如下：

中级CA名称	SCCA SSL CA1	SCCA EV SSL CA1
国家	CN	CN
组织	Sichuan Digital Certificate Authority Management Center	Sichuan Digital Certificate Authority Management Center
通用名	SCCA SSL CA1	SCCA EV SSL CA1
颁发者	SCCA Root CA1	SCCA Root CA1
颁发机构密钥标识符	2317FE4C18A9B21E30EE057EB228F9D4603CECAD	2317FE4C18A9B21E30EE057EB228F9D4603CECAD
主题密钥标识符	F9A5FEA9E976FA738B2B1CA954C6F5D3396A7B39	D059B06484F64912074CBC8C78D58025B750DC60
序列号	725CCD3E95C141A8E3CD07E8805A76A8EF483234	158361E3460BCC0D80C58F68432BDEB5650E2B6E
有效期	20 年	20 年
起始日期	2022年8月29日 16:54:21	2022年8月29日 16:55:24
到期日期	2042年8月24日 16:54:21	2042年8月24日 16:55:24
算法	SM2(256 bits)	SM2(256 bits)
签名算法	SM3withSM2	SM3withSM2

上述信任体系签发的订户证书可根据证书策略中标识的本CPS 1.2节定义的证书对象标识符进行辨别。

1.2 文档名称与标识

本文档称为《四川 CA 国密 SSL 证书电子认证业务规则》（简称本 CPS），CPS 为“Certification Practice Statement”的缩写。在本文档中，CPS 等同于本节中定义的文档名称和适用名称。

四川 CA 注册的 OID 为 1.2.156.112646，本 CPS 的对象标识符为：1.2.156.112646.1.1.2，四川CA在本CPS中为SSL证书分配的OID如下：

1）EV SSL证书策略对象标识符：1.2.156.112646.1.1.11；

2）OV SSL证书策略对象标识符：1.2.156.112646.1.1.12；

3）IV SSL证书策略对象标识符：1.2.156.112646.1.1.13；

4）DV SSL证书策略对象标识符：1.2.156.112646.1.1.14；

5）私域 SSL证书策略对象标识符：1.2.156.112646.1.1.15。

四川CA同时会使用 CA/B Forum保留的策略对象标识符。

1）EV SSL 证书策略对象标识符：2.23.140.1.1；

2）OV SSL 证书策略对象标识符：2.23.140.1.2.2；

3）IV SSL 证书策略对象标识符：2.23.140.1.2.3；

4）DV SSL 证书策略对象标识符：2.23.140.1.2.1。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构（CA）

电子认证服务机构（Certification Authority，简称CA）指所有得到授权能够颁发公钥证书的实体。四川 CA 作为电子认证服务机构，运营并维护认证体系，向订户颁发数字证书。

1.3.2 注册机构（RA）

注册机构（RA）代表 CA 建立起证书注册过程，负责对证书申请者（订户）进行身份标识和鉴别，初始化或拒绝证书申请和吊销请求，批准更新证书或更新密钥的申请。

四川CA除了承担 CA 的角色外，将自行担任 RA，不再另行设立 RA。

1.3.3 订户

订户指从四川 CA 获得数字证书的实体，可以是个人、机构或设备。订户通常需要同四川CA签订合约以获得数字证书，并承担作为证书订户的责任。

在电子签名应用中，电子签名人、证书持有人即订户。

1.3.4 依赖方

依赖方是指为某一应用而使用、信任四川CA签发的证书的实体。

依赖方可以是四川CA的证书订户，也可以不是证书订户。

1.3.5 其他参与者

其他参与者是指为四川CA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

四川CA签发的SSL/TLS服务器证书，主要用于标识Web网站或者Web服务器的身份，证明网站的身份或者资质，提供SSL/TLS加密通道，不得用于各类交易、支付的签名或验证。

四川 CA 按照所签发 SSL 证书的安全等级、鉴别方式等不同，在本 CPS 体系下签发的SSL服务器类证书分为：DV SSL（Domain Validation SSL）证书、IV SSL（Individuals Validation SSL）证书、OV SSL（Organization Validation SSL）证书和 EV SSL（Extended Validation SSL）证书。另外，还签发私域SSL证书。订户可以根据实际需要，自主判断和决定采用相应合适的证书类型。

1.4.1.1 DV SSL证书

DV SSL证书（Domain Validation SSL Certificates），即只验证网站域名所有权的简易型 SSL证书。DV SSL证书只验证网站域名所有权、控制权，不验证网站域名所有者的真实身份。DV SSL证书只提供网站机密信息的加密功能。

DV SSL证书只能是Web服务器的域名，不受理IP地址的申请，可以是单域名、多域名或通配符证书。

1.4.1.2 IV SSL证书

IV SSL证书（Individuals Validation SSL Certificates），即需要验证网站经营者个人身份的标准型SSL证书。IV SSL证书除了验证网站域名所有权、控制权，还会对网站域名所属个人的真实身份进行验证。IV SSL 证书可实现网站机密信息的加密以及网站身份的验证功能。

IV SSL证书可以包含单域名、多域名、通配符证书、公网IP证书。

1.4.1.3 OV SSL证书

OV SSL证书（Organization Validation Certificates），即需要验证网站所属机构真实身份的标准型SSL证书。OV SSL证书除了验证网站域名所有权、控制权，还会对网站域名所属机构的真实身份进行验证。OV SSL 证书可实现网站机密信息的加密以及网站身份的验证功能。

OV SSL证书可以包含单域名、多域名、通配符证书、公网IP证书。

1.4.1.4 EV SSL证书

EV SSL证书（Extended Validation SSL Certificates），即经过更加严格的身份验证后签发的一种扩展验证型服务器证书，其验证流程符合 CA/Browser 论坛制订的增强型身份验证标准（EV Guidelines）。EV SSL证书可用来验证证书中标识的域名的身份，以及持有该域名的法人机构身份。凡是经过验证后确定是由四川CA签发的EV证书，均表明该证书中所包含的信息真实有效，并且已经通过了适当且可靠的身份鉴别程序。EV SSL证书可实现网站机密信息的加密以及网站身份的验证功能。

EV SSL证书只能是Web服务器的域名，并且域名不能包含通配符，不接受理IP地址的申请，EV SSL证书可以是单域名、多域名证书。

1.4.1.5 私域 SSL 证书

私域 SSL 证书，只用于识别内网域名或内网 IP 的 SSL 证书。私域 SSL 证书只提供内网机密信息的加密功能。

私域 SSL 证书可以包含内网单域名、内网 IP 证书。

1.4.2 限制的证书应用

四川 CA 所颁发的 SSL 证书在功能上是受到限制的，只能应用于证书所代表的主体身份适合的用途。对于证书的应用超出本 CPS 限定的应用范围，将不受本 CPS 保护。

各类证书的密钥用法在订户证书中的扩展项中进行了限制。然而基于证书扩展项限制的有效性取决于应用软件，如果参与方不遵守相关约定，其对证书的应用超出本 CPS 限定的应用范围，将是不受保护的。

四川 CA 颁发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形下使用，订户不得将证书用于中间人攻击、钓鱼式攻击、欺诈网站或其他恶意犯罪行为，不得将证书用于发布任何包含或疑似包含恶意代码的程序，由此造成的法律后果由订户负责；同时，所有证书不设计用于、不打算用于、也不授权用于危险环境中的控制设备，或用于要求防失败的场合，如核设备的操作、航天飞机的导航或通讯系统、空中交通控制系统或武器控制系统中，因为它的任何故障都可能导致死亡、人员伤害或严重的环境破坏。

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 的管理机构是四川 CA 安全策略委员会，由四川 CA 安全策略委员会负责本 CPS 的制定、发布、更新等事宜。

1.5.2 联系人

1.5.2.1 证书问题报告

证书问题报告及证书撤销请求须通过以下方式提交，且证书撤销请求必须以书面形式提交。

1）发邮件至：sslservice@sicca.com.cn;或

2）致电：+86-400-028-1130。

1.5.2.2 CPS 问题

本 CPS 在四川 CA 网站发布，对具体个人和组织不另行通知。任何有关 CPS 的问题、建议、疑问等，都可以按以下方式联系。

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

邮编：610041

电话：+86-28-85336171

传真：+86-28-85336171-808

1.5.3 决定 CPS 符合策略的机构

本 CPS 由四川 CA 安全策略委员会组织制定、修订，报四川 CA 安全策略委员会批准实行。

1.5.4 CPS 批准和修订程序

本 CPS 由四川 CA 安全策略委员会负责审核并批准。如需修订，安全策略委员会组织相关人员负责修订，并报安全策略委员会批准通过，审批通过后在公司网站对外公布，自公布之日起三十日内向工业和信息化部备案。

1.6 定义与缩写

1.6.1 定义

表 1-定义

术语	定义
安全策略委员会	四川 CA 认证服务体系内的最高策略管理监督机构和 CPS 一致性决定机构
证书	是指一段信息，它至少包含了一个名字，标识特定的 CA 或标识特定的订户，它包含了订户的公钥、证书有效期、证书序列号，及 CA 数字签名。
证书申请	来自证书申请者的、要求 CA 签发证书的请求
证书申请者	要求一个发证机构签发证书的个人、组织机构或其授权代理者。

术语	定义
证书链	一个有序的证书列表，包含了订户的证书和发证机关的证书，该列表最顶级证书为根证书，最下级证书为订户的证书。
证书策略（CP）	是一个有关证书业务策略的主要说明。
证书吊销列表（CRL）	一个定期(或根据要求)发行的、并由发证机关数字签名的信息列表，用来识别在有效期内提前被吊销的证书。这个列表通常标明CRL发布者的名字，发布的日期，下一次CRL发布的日期，被吊销证书的序列号，吊销证书的时间和原因。
CA注销列表（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。
认证机构(CA)	一个授权签发、管理、吊销和更新证书的实体。
电子认证业务规则(CPS)	认证机构批准或拒绝证书申请、签发、管理和吊销证书时必须遵守的业务规则的描述。
一致性审计	一个认证机构或注册机构要定期经历的审计，通过该审计确定它是否满足有关标准。
安全损害	对安全策略的违反（或怀疑违反），包括出现敏感信息未经授权的泄漏或失去对其的控制。对于私钥，安全损害是指丢失、失窃、公开、修改、未经授权的使用或私钥受到的其它安全危害威胁。
机密/私密信息	根据CPS 9.3，9.4要求需保密的信息。
服务器证书	用于支持浏览器和服务器之间的SSL会话。该证书用于标识组织机构的Web服务器的身份，将一个域名与一台服务器绑定。该服务器证书确保服务器的拥有机构有权使用证书上的域名，确保当一个用户访问一个以该域名命名的Web服务器时，用户访问的Web服务器就是他要访问的服务器，而不是假冒的服务器，另外它可实现信息从客户端到服务器端的保密传送。
DV SSL 证书	域名验证型SSL证书，只验证网站域名所有权的简易型SSL证书。
OV SSL 证书	企业验证型 SSL 证书，既要验证网站域名所有权，也要验证网站经营者（机构）真实身份的标准型SSL证书。
IV SSL 证书	个人验证型 SSL 证书，既要验证网站域名所有权，也要验证网站经营者（个人）真实身份的标准型SSL证书。

术语	定义
EV SSL 证书	增强验证型SSL证书，需要对网站域名所有权、网站经营者及证书申请者的真实身份进行更加严格的增强型/扩展型验证，遵循全球统一的严格身份验证标准。
私域 SSL证书	只用于识别内网域名或内网IP的SSL证书。
WebTrust	针对电子认证服务机构的现行国际审计标准。
知识产权	在版权、专利、商业秘密、商标和其他知识产权下拥有的权利。
密钥生成规程参考指南	描述密钥生成规程要求和业务操作的文档。
密钥生成规程	CA 密钥对产生、其私钥被传送到密码模块、私钥备份和签发它的公钥的过程。
未经验证的订户信息	指证书申请者提交给CA或RA、并被包含在证书中的信息，但该信息未经CA或RA 证实，因此 CA 或 RA 除确认该信息是由证书申请者提出外，对其它信息不作确认。
抗抵赖	一种提供通信保护的属性，它可以防止通信一方否认信息的出处，否认它已经提交或传送了这些信息。否认出处包括否认某一通信与先前的一系列消息源来自同一地方，即使不知发送者是谁。（注：只有法院的判决、仲裁或其它的裁决才能够最终阻止抵赖。例如，合法、有效证书的数字签名是裁判所作出抗抵赖裁决的支持证据。）
在线证书状态查询协议(OCSP)	为依赖方提供实时查询证书状态信息的协议。
操作期限	指从证书签发日期和时间（或者证书上指定的一个较晚的日期和时间）开始，到证书过期或被吊销时的日期和时间为止的这段时间。
PKCS#10	公钥密码标准#10，它定义了证书签名请求的结构。
PKCS#12	公钥密码标准#12，它定义了私钥安全传送的方法。
公钥基础设施(PKI)	所有支持基于证书的公开密钥系统实施和操作体系的组织机构、技术、业务和过程的总称。
注册机构(RA)	CA 批准的一个实体，它帮助证书申请者申请证书，批准或拒绝证书申请，吊销证书或更新证书。
依赖方	信赖一个证书和/或一个数字签名的个人或组织机构。

术语	定义
依赖方协议	协议规定了一个组织机构或个人作为依赖方的条件和要求。
信息库	认证机构提供的、可在线访问的证书和其他证书有关信息的数据库。
秘密分割（秘密共享）	根据秘密分割算法，将激活 CA 私钥需要的数据分割成多个部分，使用其中若干个分割可以恢复原激活数据。
安全套接层协议(SSL)	由 Netscape 公司开发的、保护 Web 通信的一个工业标准。SSL 为一个 TCP/IP 连接提供数据加密、服务器验证、信息完整性和可选的客户端验证等。
主体	与公钥对应的私钥的持有者。在组织机构证书中，主体指的是持有私钥的设备或装置或组织机构本身。一个主体只有唯一的、确切的命名。它和该主体证书中的公钥绑定在一起。
订户	对于个人证书，订户是指人，他是证书的主体；对于组织机构身份证书，订户是指组织机构；对于组织机构代表人身份证书，订户是组织机构授权的代表人；对于服务器证书，它是证书主体所对应设备的拥有者。一个订户可以使用或被授权使用证书所含公钥对应的私钥。
订户协议	一个 CA 或 RA 拟定的协议，规定一个人或组织机构作为证书订户需要遵循的条款和条件。
可信人员	在认证机构的雇员、合同商或顾问，他们负责保证实体基础设施的可信性，以及管理产品、服务、设施和业务的可信性。
安全可信系统	是指能够有效地避免被入侵与滥用的，提供可靠的、可用的、有正确操作保障的、能够完成预定功能的、实施了适当的安全策略的计算机硬件、软件与程序。安全可信系统不一定是政府信息系统分级中所定义的“可信系统”。

1.6.2 缩写

表 2-缩写

缩写	全称
CA	认证机构
CP	证书策略
CPS	认证业务规则
CRL	证书吊销列表

缩写	全称
ARL	认证机构 CA 证书的吊销列表
OCSP	在线证书状态查询协议
OCA	运营 CA
DN	甄别名
LDAP	轻量目录访问协议
PCA	主认证机构
PIN	个人身份识别码
PKCS	公钥密码标准
PKI	公钥基础设施
RA	注册机构
LRA	证书注册受理点
RFC	请求评注标准(一种互联网建议标准)
SSL	安全套接层协议

2. 信息发布与管理

2.1 信息库

四川 CA 信息库是一个对外公开的信息库，面向订户及依赖方提供信息服务，包括不限于四川 CA 官方网站、CP、CPS、用户协议（数字证书服务协议）、依赖方协议、根证书、中级 CA 证书及认证系统的证书服务站点（LDAP、CRL 及 OCSP）。

2.2 认证信息的发布

本 CPS 发布在四川 CA 官方网站（www.scca.com.cn），供相关方获取。一经网站发布，即时生效。在四川 CA 没有发布新的 CPS，或者没有任何形式的公告、通知等形式宣布对 CPS 进行修改、补充、调整或者更新前，当前的 CPS 即处在有效的和正在实施的状态。只有四川 CA 有权利对这种状态进行任何形式的改变。

用户证书可从四川 CA 的 LDAP 服务器或证书服务站点获取；已被吊销了的证书的信息可从 CRL 站点、LDAP 查获；证书的状态信息也可通过 OCSP 服务实时查询。

2.3 发布的时间或频率

四川CA的 CPS 可通过信息库 7*24 获得，四川CA至少每年发布一次 CPS。

四川CA签发的订户证书一经签发即可下载，订户可通过邮件或四川CA提供的证书服务站点获得已签发的证书，并通过 OCSP 对证书状态进行查询。

四川CA对于订户证书的 CRL 至少每4天发布一次；对于子 CA 证书的 CRL 至少12个月发布一次，如果有子 CA 证书吊销的情况，则四川CA在24小时之内更新发布CA证书的 CRL。在紧急的情况下，信息库其他内容的发布时间和频率，由四川 CA 独立做出决定，这种发布应该是即时的、高效的，并且是符合国家法律的要求的。

2.4 信息库访问控制

四川CA信息库中的信息以只读的方式对外提供查询和获取。四川CA通过网络安全防护、系统安全设计、安全管理制度确保这些信息只有授权人员才能对信息库进行操作，如增加、删除、修改和发布信息库。

3. 身份标识与鉴证

3.1 命名

3.1.1 名称类型

四川CA颁发的数字证书符合 X.509 标准和 RFC 5280 标准。分配给证书持有者实体的甄别名（Distinguished Name），采用 X.500 标准命名方式。四川CA颁发的 SM2 SSL 服务器证书，所有的域名或 IP 地址都添加到主题别名中，而通用名为主域名或 IP 地址，必须是一个出现在主题别名中的域名或 IP 地址。

3.1.2 对名称意义化的要求

订户证书所包含的名称具有一定的代表性意义，其中包含的主体识别名称，应当能够明确确定证书持有机构以及所要标识的网络主机服务器、或互联网域名，并且可以被依赖方识别。主体识别名称应当符合法律法规等相关规定的要求。

3.1.3 订户的匿名或伪名

本 CPS 所述证书的订户在进行证书申请时不能使用匿名或伪名。

3.1.4 理解不同名称形式的规则

四川CA签发的数字证书符合 X.509 V3 标准，甄别名格式遵守 X.500 标准。

3.1.5 名称的唯一性

四川CA签发给某个实体的证书，其主体甄别名，在该证书签发CA信任域内是唯一的。但对于同一订户，四川CA可以用其唯一的主体甄别名为其签发多张证书。

3.1.6 商标的识别、鉴证和角色

四川 CA 签发的证书不包含任何商标，不验证申请人的商标使用权。当发生商标纠纷时，四川CA有权拒绝证书申请和吊销已签发的证书。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

证书申请者必须证明持有与所要注册公钥相对应的私钥，证明的方法是在证书申请消息中包含数字签名（PKCS#10）。

3.2.2 订户身份和域名的鉴别

3.2.2.1 OV SSL 订户身份的鉴别

OV SSL 证书只接受以组织机构身份申请，可以包含单域名、多域名、通配符证书、公网IP证书。

签发OV SSL证书时，四川CA对订户的组织机构进行身份鉴证，鉴证方法包括：

- 确认组织机构是确实存在的、合法的实体。确认的方式可以是面对面审查组织机构成立的有效文件，如营业执照、组织机构代码证、事业单位法人证书、社会团体登记证书、民办非企业登记证书等，通过权威第三方数据库确认；或通过组织机构的银行账户转账等方式验证组织机构真实性。

- 授权申请人应提交当前有效的政府签发的身份证件（身份证、护照等），四川 CA 将通过认可的提供身份证真实服务的数据库中信息，如公安部门提供的个人身份数据库、电信运营商身份库、政府机构及信用机构或其他可靠的信息源；或个人网银转账信息确认授权申请人身份真实性。
- 确认该组织机构知晓并授权证书申请，即代表组织机构提交证书申请的人是经过授权的。确认的方式可以是：
  - 使用从网络或其它常规途径获取验证电话号码，进行电话验证，获得组织机构有关申请及授权事宜的确认；
  - 由该机构提供加盖公章的授权信函、传真确认。

3.2.2.2 IV SSL 订户身份的鉴别

IV SSL 证书只接受以个人身份申请，可以包含单域名、多域名、通配符证书、公网IP 证书。

签发 IV SSL 证书时，四川 CA 对订户个人进行身份鉴证，鉴证方法包括：

- 确认证书申请者提交的身份信息确实存在且正确，个人身份的鉴别除采用受理点现场鉴别外，还可通过在线电子化的方式进行鉴别。具体方法包括：
  - 订户应提交当前有效的政府签发的身份证件（身份证、护照等），采用四川 CA 认可的、提供身份证真实服务的数据库中的信息，如公安部门提供的个人身份数据库、电信运营商身份库、政府机构及信用机构或其他可靠的信息源；或个人网银转账信息确认申请者身份真实性。
- 验证证书申请者是证书申请中所说的那个人，验证的方式包括：
  - 验证申请者知晓或拥有通常只有真正的申请者才知晓或拥有的秘密，如通过订户银行帐户进行转帐验证；
  - 其他安全可靠的方式体现申请人真实意愿，如视频语音、面对面等；
  - 对于委托他人进行申请的，要提交被充分授权的书面证明文件。

3.2.2.3 EV SSL 订户身份的鉴别

EV SSL 证书只接受以组织机构身份申请，可以包含单域名、多域名；域名不能包含通配符；不受理 IP 地址申请。

签发 EV SSL 证书时，四川 CA 除对订户组织机构身份进行本 CPS 3.2.2.1 标准型鉴证外，还对订户组织机构身份进行以下增强型鉴证。

- EV SSL 申请者合法存在及身份鉴别

对于 EV SSL 证书，四川 CA 将与注册机构核实申请者的合法存在和身份。通过查询申请机构社会统一信用代码、企业年报及营业执照，验证申请机构身份信息、经营地址及注册地址。

- EV SSL 证书申请者业务存在核实

四川 CA 通过以下方式之一验证申请人具有从事业务的能力：

  - 核实申请人、关联公司、母公司或子公司已存在至少三年；
  - 使用已验证的律师信，表明申请人在受监管的金融机构拥有活跃的活期存款账户。

- EV SSL 证书使用者字段要求

subjectorganizationName (OID 2.5.4.10)字段中包含由 3.2.2.1 中的方式鉴证的申请者的完整合法组织名称；

subjectbusinessCategory (OID 2.5.4.15)字段中包含以下字符串之一：“Private Organization”，“Government Entity”，“Business Entity”，or “Non-Commercial Entity”；当 subjectbusinessCategory (OID 2.5.4.15)字段中包含内容为“Business Entity”时，证书主体为个体工商户，证书申请人需是经营者本人，必须经过“面对面”（视频）的方式进行验证；

subjectjurisdictionLocalityName (OID 1.3.6.1.4.1.311.60.2.1.1)，subjectjurisdictionStateOrProvinceName (OID 1.3.6.1.4.1.311.60.2.1.2)，subjectjurisdictionCountryName (OID 1.3.6.1.4.1.311.60.2.1.3)字段中，包含注册机构的司法管辖区级别，四川 CA 已将这些字段中的值在官网最新公开的鉴证信息来源中披露；

subjectserialNumber (OID 2.5.4.5)字段中包含统一社会信用代码，四川CA已将本字段中可接受的注册号格式在官网最新公开的鉴证信息来源中披露；

四川CA签发的 EV SSL 证书不包含经营别称DBA（DBA是Doing Business As的缩写，是指任何不同于公司注册名称的其他经营别称）。

- EV SSL 相关申请人员角色

EV SSL 证书的申请者只能是国家机关、企事业单位、社会团体等机构订户，申请机构必须拥有如下角色：

申请人：申请单位经办人员；

审批人：申请单位主管人员；

签署人：申请协议的签署人。

证书申请机构可授权一人或多人完成所有角色，四川 CA 将通过拨打电话（通过3.2.2.9 中可靠数据源得到的公司电话）与申请机构联系，确定申请人、审批人、签署人的人员身份及授权。四川 CA 将使用同样方式验证证书申请及订户协议上的签名为真实有效。

- EV 鉴证职责分离

在所有验证过程和程序完成后，四川 CA 将由一个不负责收集信息的人员审查所有为支持 EV 证书申请而收集的信息和文件，并批准签发 EV SSL 证书。

3.2.2.4 DBA/商业名称的鉴别

不适用。

3.2.2.5 国家的鉴别

如果四川CA签发的证书主题中包含国家代码，则四川CA通过下列方法中的一种或多种方式进行验证：

1）从 DNS 记录中获取到的 IP 地址所在国家；

2）申请域名的 CCTLD。

3）通过查询政府机构或其他可信第三方数据源确认申请者的地址所在的国家。

3.2.2.6 域名的确认和鉴别

四川CA将对在证书中列出的所有域名进行所有权的验证。四川CA不会将域名所有权验证委托给任何第三方进行。对于域名的验证，被验证的实体可以是订户的母公司、子公司或联营公司，四川CA通过以下方式之一来确认域名权限：

1）通过邮件、短信或邮寄邮件方式发送随机值，然后接收一个使用该随机值的确认响应，确认申请人对全限定域名FQDN(Fully Qualified Domain Name)的所有权。随机值必须发送到标识为域名联系人的电子邮件地址或'admin'，'administrator'，'webmaster'，'hostmaster'或'postmaster'，后面是（“@”）之后跟着授权域名、电话号码或邮件地址。一旦使用此方法验证了对 FQDN 的所有权，CA 也可为其他相同顶级域名颁发证书。

2）通过在“/.well-known/pki-validation”目录下对约定的信息进行改动，确认订户对 FQDN 的所有权。

3）通过在 DNS CNAME、TXT 记录中是否存在已约定的随机值，以确认订户对域名的所有权。一旦使用此方法验证了对 FQDN 的所有权，CA 也可为其他相同顶级域名颁发证书。

4）域名注册信息应公开在WHOIS 数据库，包括申请机构名称、地址和联系方式。

通过域名注册信息查询(whois)功能。得到所申请域名证书的域名注册者资料，查看域名注册者是否和域名证书申请者一致，初步审核确定域名证书申请者确实拥有此域名。如域名申请者与在(whois)查询到的结果不一致或域名持有者关闭相关信息,则订户可提供授权证明或者四川CA采取邮件方式询问是否授权给证书申请者使用。

5）通过在第三方数据源中查询域名所有者，确认订户对域名的所有权。此方法仅限用于验证私域 SSL 证书。

6）由域名所有者提供域授权的信件或其他文件，证明订户有权为特定域名空间申请证书。此方法仅限用于验证私域 SSL 证书。

7）对于内部名称，订户需提供域名所有权声明函。此方法仅限用于验证私域 SSL 证书。

3.2.2.7 IP地址的确认和鉴别

四川CA在此 CPS 体系下不为 IANA 标注的 Reserved IP 签发证书。

四川CA将对在证书中列出的所有 IP 进行所有权的验证。四川CA通过以下方式之一来确认 IP 权限：

1）订户提交ISP 商分配 IP 的纸质盖章证明材料或者ISP 的邮件证明材料。

2）通过在“/.well-known/pki-validation”目录下对约定的信息进行改动，确认订户对 IP 的控制权。

3）通过邮件、短信或邮寄邮件方式发送随机值，然后接收一个使用该随机值的确认响应，确认申请人对 IP 的控制权。随机值必须发送到标识为 IP 联系人的电子邮件地址、电话号码或邮件地址。

4）通过 IP 地址上的反向 IP 查找获得与 IP 地址关联的域名，然后使用第3.2.2.6节允许的方法验证对 FQDN 的控制，确认申请人对 IP 地址的控制。

5）通过拨打标识为IP联系人的电话号码并获得确认申请人验证 IP 地址请求的响应，确认申请人对IP地址的控制。

6）对于 Intranet IP，订户需提供IP地址使用权承诺函。此方法仅限用于验证私域SSL 证书。

3.2.2.8 通配符域名的确认和鉴别

对于通配符域名，四川 CA 验证通配符右侧的域名。确保该域名是明确归属于某一商业实体、社会组织或政府机构等机构，并经过合法的注册获得的。

四川 CA 拒绝通配符右侧的域名直接是顶级域名、公共后缀或由域名注册管理机构控制的域名申请证书，除非订户能够证明其完全控制该域名的所有命名空间。

必要时，四川 CA 需采取其他独立的审核方法，以确定域名的归属权，如需要订户提供相应的协助，订户不能以任何理由拒绝这种请求。

3.2.2.9 数据源及其准确性

3.2.2.9.1 鉴证数据源

四川 CA 将鉴证数据来源（注册机构及查询方式等）在官方网站上公布，如有需要，请访问 https://www.scca.com.cn/。

四川CA在使用新的鉴证数据来源之前，将首先在此文件中进行更新披露。

3.2.2.9.2 数据源准确性

在使用任何数据源作为可靠的数据源之前，四川 CA 对该来源的可靠性、准确性，及更改或伪造可抗性进行评估，并考虑以下因素：

1）所提供信息的使用年限；

2）信息来源的更新频率；

3）数据提供者和数据收集的目的；

4）公众对数据可用性的可访问性；

5）伪造或改变数据的相对难度。

四川CA将从权威第三方数据提供机构获取数据，并进行 3.2 章节的鉴证工作。

3.2.3 没有验证的订户信息

四川CA签发的证书不包含未经验证的订户信息。

3.2.4 授权的确认

如果订户申请的证书包含的主体身份信息是一个组织，四川CA会使用第 3.2.2 中列出的来源来验证可靠的通讯信息，并使用这个信息与订户代表或在订户组织内的权威来源（包括但不限于订户的主要营业部、公司办公室、人力资源部门）确认证书申请的真实性。

如果订户以书面形式指定了证书申请的个人，则四川 CA 将不接受任何超出本规范的证书请求。四川CA可以请订户提供经其核实并盖章的书面授权信函。

3.2.5 互操作准则

截止目前，四川CA未签发任何交叉认证的证书。

3.3 密钥更新请求的标识与鉴证

3.3.1 常规的密钥更新的标识与鉴证

四川 CA 支持在有效期内的证书订户进行密钥更新请求，订户可以选择生成一个新的密钥对来替换正在使用的密钥对或即将到期的密钥对。

收到密钥更新请求后，四川 CA 会使用订户提交的新请求创建一个新的证书，新证书内容与旧证书的主题信息保持一致，证书的有效期与原证书相同。

3.3.2 吊销之后的密钥更新的标识与鉴证

四川CA对吊销后证书不进行密钥更新。

3.4 吊销请求的标识与鉴证

在四川 CA 的证书业务中，证书吊销请求可以来自订户，依赖方，应用软件供应商。另外，当四川CA认为必要的时候（参见本 CPS 第 4.9.1 节所述相关情形），有权发起吊销订户证书。

订户通过一定的方式，如邮件、传真、电话等，向四川CA提交请求，四川CA通过与证书保障级别相应的通讯方式与订户联系，确认要吊销证书的人或组织确实是订户本人，或者其授权者。依据不同的环境，通讯方式可以采用下面的一种或几种：电话、传真、e-mail、邮寄或快递服务。

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

证书申请者可包含个人、企业单位、机关事业单位以及社会团体等各类组织机构。

4.1.2 注册过程与责任

申请者应事先了解订户协议、四川CA CPS 等文件约定的事项，特别是其中关于证书适用范围、权利、义务和担保的相关内容。

申请者应向四川CA递交 SSL 证书申请表及相应证明文件，此行为即意味着申请者已经了解和接受上述内容。

申请者应自行产生密钥对，产生 PKCS#10 证书请求文件并递交给四川CA，并支付相应费用。

订户有责任向四川CA提供真实、完整和准确的证书申请信息和资料。

四川 CA 承担对订户提供的证书申请信息与身份证明资料的一致性检查工作，同时承担相应审核责任。

根据《中华人民共和国电子签名法》的规定，申请者未向四川 CA 提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、四川 CA 造成损失的，承担相应的法律及赔偿责任。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

当四川CA及其注册机构接受到订户的证书申请后，应按本 CPS 第 3.2 节的要求，对订户进行身份识别与鉴别。

四川 CA 会根据或之前由于怀疑网络钓鱼或其他诈骗用途或顾虑而拒绝的证书请求或吊销的证书，建立和维护 SSL 证书高风险数据库列表，对于OV、IV、EV证书，在接受证书申请时将会查询该列表信息。对于列表中出现的订户，四川CA将执行额外的验证。

四川 CA 验证订户提交的申请材料后，根据验证结果决定接受、拒绝该申请或要求申请者补充递交相关材料。四川 CA 在处理证书申请过程中，将通过有效手段确保证书信息与正确的申请信息相符，并将证书签发给正确的申请者。

在证书签发前，若四川CA根据本 CPS 第 3.2 节指定来源获得的数据或证明文件不超过 398 天且该信息未发生变化，则四川 CA 可重复使用该鉴证数据或证明文件，核实OV、IV、EV和私域 SSL 证书中的信息。对于 DV 证书，四川CA不重复使用鉴证数据。

4.2.2 证书申请批准和拒绝

完成本 CPS 第 4.2.1 节识别与鉴别的执行后，四川CA可根据鉴证结果批准或拒绝申请。如果拒绝申请，则应该通过适当的方式、在合理的时间内通知 SSL 证书申请者。

如果四川 CA 认为签发证书可能会给四川 CA 带来争议、法律纠纷或者损失，四川 CA 也可能拒绝证书申请。

对于法律法规、国家政府部门、行业监管部门或当地政府明确禁止从事商业活动或其它公开活动的机构，四川 CA 有权拒绝为其签发 SSL 证书。

4.2.2.1 证书申请的批准

如果符合下述条件，四川 CA 可以批准证书申请：

1) 根据本 CPS 第 3.2 节的规定，已经成功识别和认证所有必需的订户信息；

2) 订户接受或者没有反对订户协议的内容和要求；

3) 订户已经按照规定支付了相应的费用。

4.2.2.2 证书申请的拒绝

如果发生下列情形，四川 CA 有权拒绝证书申请：

1) 根据本 CPS 第 3.2 节的规定，不能完成识别和认证所有必需的订户信息；

2) 订户不能根据要求提供所需要的身份证明材料；

3) 订户反对或者不能接受订户协议的有关内容和要求；

4) 订户没有或者不能够按照规定支付相应的费用；

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

对于拒绝的证书申请，四川 CA 通知申请者证书申请失败。

4.2.3 处理证书申请的时间

四川 CA 在收到证书请求的合理时间内开始处理证书申请，在客户提交的申请资料齐全的情况下，四川 CA 将在 5 个工作之内完成证书申请处理。

4.3 证书签发

4.3.1 证书签发中 RA 和 CA 的行为

四川 CA 的根 CA 在签发证书时，要求四川 CA 授权的内部可信角色，经过严格的审批流程后，直接进行证书签名操作。

四川 CA 在签发订户证书前，将确保注册机构已对所接收的证书申请的真实性完成验证。

使用 CA 进行证书签发时，RA 会将证书申请信息打包为数据包，在对数据包进行签名和加密后，将其发送给 CA。CA 通过验证数据包上的签名，鉴别数据包的完整性，并根据签名者的信息鉴别发送者的身份和权限。鉴别通过后，CA 将使用私钥对证书申请签名生成订户证书。

4.3.2 CA 和 RA 对订户的通知

四川 CA 的证书签发系统签发证书后，将直接或者通过 RA 通知订户证书已被签发，并告知订户如何获得证书。

4.4 证书接受

4.4.1 构成接受证书的行为

在订户发生以下任意一种行为后，四川 CA 认为订户接受了证书：

1) 订户下载或安装了证书；

2) 四川 CA 注册机构在订户的允许下，代替订户下载证书，并把证书通过邮件方式发送给订户；

3) 在四川 CA 将证书获取通知发送给订户后，在 24 小时内订户未表示拒绝。

4.4.2 CA 对证书的发布

四川 CA 把证书发给订户视为证书的发布。

4.4.3 CA 对其他实体的通告

对于签发的证书，四川 CA 及其注册机构不通知其他实体。

4.5 密钥对和证书使用

密钥对和证书不应用于其规定的、批准的用途之外的目的，否则其应用是不受相关法律和四川 CA 本 CPS 的保障。

4.5.1 订户私钥和证书使用

订户在提交了证书申请并接受了四川 CA 所签发的证书后，均视为已经同意遵守与四川 CA、依赖方有关的权利和义务的条款。密钥对和证书不应用于其规定的、批准的用途之外的目的。

订户应保护其私钥避免未经授权的使用，并且不再使用过期或被吊销的证书。订户以外的各方不得存档订户的私钥。

4.5.2 依赖方公钥和证书使用

依赖方应在依赖证书前考虑总体情况和损失风险。

当依赖方接收到加载数字签名的信息后，有义务进行以下确认操作：

1) 获得数字签名对应的证书及信任链；

2) 确认该签名对应的证书是依赖方信任的证书；

3) 通过查询 CRL 或 OCSP 确认该签名对应的证书是否被吊销；

4) 证书的用途适用于对应的签名；

5) 使用证书上的公钥验证签名；

6) 考虑本 CPS 或其它地方规定的其它信息；

以上条件不满足的话，依赖方有责任拒绝签名信息。

4.6 证书更新

证书更新是指在订户证书到期之前，证书的主题信息不发生改变的情况下，为订户签发一张新证书。

4.6.1 证书更新的情形

对于四川CA签发的订户证书，证书到期前 30 天起可进行证书更新。到期前 30 天内，订户可访问四川CA证书服务站点或到注册机构进行证书更新的申请。对于 SSL 证书，四川CA接受订户在不更新密钥时申请更新证书。

4.6.2 请求证书更新的实体

同 4.1.1。

4.6.3 证书更新请求的处理

同4.2。

4.6.4 签发新证书时对订户的通知

同4.3.2。

4.6.5 构成接受更新证书的行为

同4.4.1。

4.6.6 CA对更新证书的发布

同4.4.2。

4.6.7 CA对其他实体的通告

同4.4.3。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

同3.3。

4.7.2 请求证书密钥更新的实体

同4.1.1。

4.7.3 证书密钥更新请求的处理

四川CA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，参见本 CPS第4.6.3 节的描述。

4.7.4 签发新证书时对订户的通知

同4.3.2

4.7.5 构成接受密钥更新证书的行为

同4.4.1。

4.7.6 CA对密钥更新证书的发布

同4.4.2。

4.7.7 CA对其他实体的通告

同4.4.3。

4.8 证书变更

4.8.1 证书变更的情形

证书变更是指现有证书中的主题信息不变，证书有效期不变，其他信息发生变化而申请颁发新证书。当证书变更时，四川 CA 会对证书信息进行重新验证，如果证书申请资料在可用期内（即申请资料及鉴证数据在 398 天之内），则可以直接使用申请资料，四川 CA 仅对发生变化的信息进行鉴证。若上述证书申请资料超过最大有效期则不能进行证书变更。

4.8.2 请求证书变更的实体

只有在有效期内的证书订户或证书订户的授权代表可以请求证书变更。四川 CA 不向所有订户提供证书修改服务。

4.8.3 证书变更请求的处理

同4.2。

4.8.4 签发新证书时对订户的通告

同4.3.2。

4.8.5 构成接受变更证书的行为

同4.4.1。

4.8.6 CA对变更证书的发布

同4.4.2。

4.8.7 CA对其他实体的通告

同4.4.3。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

当发现以下情况之一时，四川CA将在 24 小时之内将证书吊销：

1) 订户以书面形式请求吊销证书；

2) 订户通知四川CA最初的证书请求未得到授权且不追加授权行为；

3) 四川CA获得了证据，证明与证书公钥对应的订户私钥遭到了损害；

4) 四川CA获得证据，证书中所包含的域名或 IP 地址的控制权验证已不再可靠；

5) 四川CA获得了证书遭到误用的证据；

6) 四川CA获悉订户违反了订户协议、CP、CPS 中的一项或多项重大责任；

7) 四川CA获悉任何表明 FQDN 或 IP 地址的使用不再被法律许可（例如，某法院或仲裁员已经吊销了域名注册人使用域名的权力，域名注册人与申请人的相关许可及服务协议被终止，或域名注册人未成功更新域名）；

8) 四川CA获悉某通配符证书被用于鉴别具有欺骗误导性的子域名；

9) 四川CA获悉证书中所含信息出现重大变化；

10) 四川CA获悉证书的签发未能符合本 CPS 要求；

11) 四川CA认为任何出现在证书中的信息不准确、不真实或具有误导性；

12) 四川CA由于任何原因停止运营，且未与另一家 CA 达成协议以提供证书吊销服务；

13) 四川CA签发证书的权力失效，或被吊销或被终止，除非其继续维护 CRL、OCSP 信息库；

14) 四川CA的 CP 或 CPS 要求吊销订户证书；

15) 四川 CA 发现了已经被论证的方法证明订户的私钥被泄漏，该方法可以通过公钥简单的计算出私钥，或者有明确的证据证明订户用来生成私钥的方法是有缺陷的；

16）CPS 中职责的履行被延迟或受不可抗力的阻碍；自然灾害；计算机或通信失败；法律、规章或其它法律的改变；政府行为；或其它超过个人控制的原因并且对他人信息构成威胁的；

17）四川CA已经履行催缴义务后，订户仍未缴纳服务费。

4.9.2 请求证书吊销的实体

请求证书吊销的实体可为订户、四川 CA 及其注册机构、或经司法机构授权的司法人员。此外，依赖方、应用软件提供商，防病毒机构或其他的第三方可以提交证书问题报告，告知四川CA有合理理由吊销证书。

4.9.3 吊销请求的流程

4.9.3.1 订户主动提出吊销申请

1）订户向四川CA提交吊销申请表和身份证明材料，同时说明吊销原因；

2）四川CA按照本 CPS 第 3.4 节的规定进行证书吊销请求的鉴别；如鉴证通过则进行吊销处理。

3）四川CA完成吊销后及时将其发布到证书吊销列表；

4）四川CA通过电话、邮件等适当方式，通知订户证书被吊销及被吊销的理由；若未能联络订户时，在必要的情况下，四川CA对吊销的证书将通过网站进行公告；

5）四川CA提供 7x24 小时的证书吊销申请服务，订户可通过四川CA官方网站公布的联系方式申请证书吊销。

4.9.3.2 订户被强制吊销证书

1）当四川CA有充分的理由确信出现本 CPS 第 4.9.1 节情形时，四川CA将通过内部流程申请吊销证书；

2）在四川CA的根证书或中级 CA 证书相对应的私钥出现安全风险时，经国家电子认证服务主管部门批准后可直接进行订户证书吊销；

当依赖方如司法机构、应用软件提供商、防病毒机构等第三方提请证书问题报告时，四川 CA 应组织调查并根据调查结果来决定是否吊销证书，如果通过调查确认证书需要吊销，则从收到证书问题报告到证书吊销不超过 4.9.1 中规定的期限；

3) 在证书吊销后，四川 CA 或注册机构将通过适当的方式，包括邮件、电话等，通知最终订户证书已被吊销及被吊销的理由；若未能联络订户时，在必要的情况下，四川 CA 对吊销的证书将通过网站进行公告。

4.9.4 吊销请求宽限期

四川 CA 不支持吊销请求宽限期。

4.9.5 CA 处理吊销请求的时限

四川 CA 将在接到证书问题报告的 24 小时内，对证书问题报告内容进行调查，以决定是否吊销或采取其它适当的行动处理机制。

如果四川 CA 通过调查确认证书需要吊销，则从收到证书问题报告到证书吊销不超过 4.9.1 中规定的期限。

4.9.6 依赖方检查证书吊销的要求

依赖方应当检查他们所信任的证书是否被吊销。检查方式是通过查询四川 CA 提供的 OCSP 服务或 CRL 查询。

4.9.7 CRL 发布频率

对于订户证书，四川 CA 的 CRL 发布周期不超过 96 小时，即在 4 天内发布最新 CRL。订户 CRL 的有效期最长不会超过 7 天。

对于中级 CA 证书，四川 CA 的 CRL 发布周期不超过 12 个月。如果吊销中级 CA 证书，四川 CA 在吊销后 24 小时之内更新 CRL。中级根 CRL 的有效期最长不会超过 12 个月。

4.9.8 CRL 发布的最大滞后时间

四川 CA 的 CRL 发布最大滞后时间为 CRL 签发之后的 24 小时内。

4.9.9 在线状态查询的可用性

四川CA向证书订户和依赖方提供在线证书状态查询服务。四川CA的 OCSP 服务符合RFC6960 的要求。

4.9.10 在线状态查询要求

用户可以自由进行在线状态查询，四川CA没有设置任何的查询限制。

对于订户证书，四川CA至少每4天更新OCSP信息，OCSP 响应的最长有效期为7天。

对于中级 CA 证书，四川CA至少每12个月更新OCSP信息。当吊销中级CA证书时，四川CA会在24小时内更新OCSP信息。

4.9.11 吊销信息的其他发布形式

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。

4.9.12 密钥损害的特别要求

无论是订户还是注册机构，发现证书密钥受到安全损害时，应立即向四川 CA 提出吊销证书的请求。

如果 CA 的密钥（根 CA 或中级 CA 密钥）安全被损害或者怀疑被损害，四川CA将在合理的时间内用合式的方式及时通知订户和依赖方。

4.9.13 证书挂起的情形

四川CA不支持证书挂起。

4.9.14 请求证书挂起的实体

不适用。

4.9.15 挂起请求的流程

不适用。

4.9.16 挂起的期限限制

不适用。

4.10 证书状态服务

四川CA通过 CRL 和 OCSP 提供证书状态查询服务，并确保对查询请求有合理的响应时间和并发处理能力。

4.10.1 操作特征

对于被吊销的证书，四川CA在该证书到期前不删除其在 OCSP 服务器中的吊销记录；在该证书到期前不删除其在 CRL 中的吊销记录。四川CA的证书状态查询以网络服务的形式提供：

- CRL 采用 HTTP 协议提供；
- OCSP 符合 RFC6960。

4.10.2 服务可用性

四川CA的 CRL、OCSP 证书状态服务均为 7x24 可用，且会最大限度地减少停机时间。响应时间不超过 10 秒，即：在网络允许的情况下，订户和依赖方能够实时获得证书状态查询服务的响应。

4.10.3 可选特征

无。

4.11 订购结束

订购结束包含以下情况：

1）证书到期后没有进行更新；

2）证书到期前被吊销。

一旦用户在证书有效期内终止使用四川CA的证书认证服务，四川CA在批准其终止请求后，将实时把该订户的证书吊销，并按照 CRL 发布策略进行发布；四川CA详细记录吊销证书的操作过程并定期将订购结束后的证书及相应订户数据进行归档。

4.12 密钥托管与恢复

四川CA不托管任何 SSL 证书订户的私钥，因此也不提供密钥恢复服务。

4.12.1 密钥托管与恢复的策略与行为

不适用。

4.12.2 会话密钥的封装与恢复的策略与行为

不适用。

5. 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

四川 CA 的运营机房位于成都市双流区物联一路 788 号中国联通四川天府信息中心 C 栋 1 楼 C101 室。

运营机房按照国家相关规范进行构建，整体建筑由能够阻止物理穿透的材料建成。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、穿透。根据消防要求设置了烟感、温感以及气体消防设备。

运营机房场地的物理安全是基于物理层级的保护，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。

运营机房场地能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。

5.1.2 物理访问控制

四川 CA 运营机房物理场地划分为公共区、管理区、服务区和核心区四个安全区域。其中公共区为机房入口之外的区域；管理区为机房运营管理的区域，包括：运维监控室、安全监控室、机房管理区；服务区为证书注册、目录服务等系统设备运行的区域；核心区

为证书签发、密钥管理等系统设备运行的屏蔽室区域。机房物理场地进入各区域的顺序，依次为公共区、管理区、服务区、核心区。

门禁系统可实现对各层门进出的控制，具备以下功能：

- 系统采用身份识别卡和指纹鉴别的控制方法，控制各个区域的进出；
- 不同级别区域门禁可设置不同种类验证因素；
- 人员进出各门禁都会有日志记录；
- 所有的门都设有强行开启报警和门开超时报警；
- 服务区和核心区安装了移动报警器，防止任何未经允许的人员滞留在房间内；
- 核心区屏蔽门实现多门互锁，防止电磁信息泄漏；
- 整套访问控制系统接入UPS配电柜，保证供电可靠性。

整个区域配置有视频监控系统，对场地内的各区域实行 7x24 小时不间断录像。所有录像资料保留不少于6个月，以备查询。

5.1.3 电力与空调

四川CA运营机房有安全、可靠的电力供电系统及电力备用系统以确保系统7x24小时正常供电及在供电系统出现供电中断时能够提供正常的服务。

供电系统为两路UPS机组，当市电停电时，UPS蓄电池满负载放电可支持设备运行15分钟以上。备用电力配置有柴油发电机组，柴油发电机组日常处于低功率运行状态。当机房出现市电停电故障时，柴油发电机组立即切换至主路并提高运行功率，15 分钟内供电能完全切换至柴油发电机组，保证机房电力的不间断供应，柴油库中存储油量可支撑满负载运行8小时以上。

四川 CA 运营机房配置有新风系统和多台柜间水冷空调系统，控制运营设施中的温度和湿度处于正常范围内。

5.1.4 水患防治

四川 CA 运营机房中各水冷柜间空调底部四周均安装有专门的漏水检测装置，并接入运营机房环境控制系统中，能够及时发现和告知漏水情况。

5.1.5 火灾防护

四川 CA 运营机房由第三方检测机构对机房整体建筑消防设施进行竣工验收检测，检测结果满足 GA503-2004《建筑消防检测技术规程》要求。

- 四川 CA 运营机房设施内设置火灾报警装置。在机房内设置烟、温感探测器。
- 机房区域内均配置了独立的气体灭火装置。
- 各区域隔断均采均用符合检测要求的防火门或屏蔽门。
- 各道门禁处均设置有应急照明以及疏散指示标志。

5.1.6 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）。

5.1.7 废物处理

四川 CA 对不再使用的纸质敏感文件和材料均进行物理销毁；存储介质按照保密级别采用软件或者物理方式进行信息清除，确保信息无泄漏风险。加密设备在作废处置前根据制造商提供的方法先将其初始化再进行物理销毁。

5.1.8 异地备份

四川 CA 对关键系统数据、审计日志数据进行异地备份，该备份地点的安全级别不低于实际生产环境。

5.2 程序控制

5.2.1 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：

- 安全管理类人员：安全策略管理组织负责人员、财务管理人员、可信雇员管理人员、安全经理，运营审计人员，密钥管理人员、服务质量管理人员；

- 运行维护类人员：物理环境维护人员、网络维护人员、系统维护人员、数据库维护人员；
- 客户服务人员：业务咨询服务人员、业务办理服务人员、鉴证服务人员、技术支持服务人员、客户档案管理人员、客户培训人员、法务人员；
- 专业技术人员：产品研发人员、项目实施人员。

5.2.2 每项任务需要的人数

四川 CA 有严格的策略和控制程序，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。

- 访问屏蔽机房需要至少两名有访问权限的人员。
- 加密设备的管理权限按照 5 选 3 方式进行分割，并由不同可信人员持有。
- 保存根密钥激活数据的保险柜设置为双人开启模式。

5.2.3 每个角色的识别与鉴别

对于可信人员的物理访问，四川 CA 通过门禁卡、指纹识别鉴别不同人员，并确定相应的权限。

对于进行订户证书生命周期管理的四川 CA、注册机构的可信人员，他们使用相应的数字证书访问系统，完成证书管理工作。

对于系统维护人员，他们使用各自的账号和密码通过堡垒机登录系统进行维护工作。

5.2.4 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：

- 数据库管理人员
- 系统管理人员
- 密钥管理人员
- CA 系统操作人员与审计人员不可兼任
- RA 业务操作的录入人员与审核人员不可兼任

5.3 人员控制

5.3.1 资格、经历和无过失要求

四川CA对承担可信角色的工作人员的资格要求如下：

1）具备良好的社会和工作背景；

2）遵守国家法律、法规，无违法犯罪记录；

3）遵守四川CA有关安全管理的规范、规定和制度；

4）具有认真负责的工作态度和良好的从业经历；

5）具备良好的团队合作精神。

5.3.2 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 将对雇佣的人员先进行背景调查。背景调查符合法律法规的要求，尽可能地通过相关组织、部门进行人员背景信息的核实，并保护个人隐私。

5.3.3 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。
- 服务流程与要求。

- 安全操作流程（系统、密钥）。

5.3.4 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一次公司安全管理策略、相关技能知识的培训。

5.3.5 工作岗位轮换周期和顺序

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。

5.3.6 未授权行为的处罚

四川 CA 对于未授权行为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。

5.3.7 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。

5.3.8 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。

5.4 审计日志程序

5.4.1 记录事件的类型

四川CA对如下几类事件进行记录：

- CA密钥生命周期内的管理事件，包括，
  - 密钥生成，备份，存储，恢复，归档和销毁。
  - 密码设备的采购、使用、归档和销毁。

这些记录都是密钥管理员完成的纸质记录。

- CA和订户证书生命周期内的管理事件，包括，
  - 证书的申请、批准、更新、吊销等。

  这些记录由认证系统自动记录，保存在数据库。
- 系统事件，包括，
  - 配置变更申请及记录、故障处理记录
  - 防火墙日志、入侵防护日志及系统运行日志

  这些记录由运维人员完成纸质记录，日志类由系统自动记录。
- 四川CA物理设施的访问记录，如，
  - 权限分配及访问记录。
  - 访问日志。

  权限分配及访问记录由管理人员完成纸质记录，访问日志由系统自动记录。

上述日志信息包括记录时间、序列号、记录的实体身份、日志种类等。

5.4.2 处理日志的周期

对于“5.4.1记录事件的类型”中的日志记录，四川CA每两个月进行一次内部检查、审计。

5.4.3 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。

5.4.4 审计日志的保护

四川CA的系统日志备份到日志服务器，纸质记录归档保存。

四川 CA 采取了物理和逻辑的访问控制方法，以确保只有授权人员才能接触这些审查记录，严禁未授权的访问、阅读、修改和删除等操作。

5.4.5 审计日志备份程序

四川 CA 的系统日志实时同步到日志服务器进行备份，业务审计记录存于数据库，随数据库每日备份，审计日志纸质记录每年进行归档。

5.4.6 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。

5.4.7 对导致事件主体的通知

当四川 CA 发现被攻击时，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。

四川 CA 有权决定是否对事件相关实体进行通知。

5.4.8 脆弱性评估

四川 CA 每月对系统进行一次漏洞扫描，每年进行一次渗透测试，同时根据审计发现的安全事件，四川 CA 将每年对系统、物理场地、运营管理等方面进行安全脆弱性评估，并根据评估报告采取措施，以降低运营风险。

5.5 记录归档

5.5.1 归档记录的类型

四川 CA 对 5.4.1 所述记录类型进行归档。

5.5.2 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，其归档应保留到完成安全脆弱性评估或一致性审计。

- 对订户证书生命周期内的管理事件的归档不少于证书失效后 5 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。
- 订户证书的归档保留期限不少于证书失效后 5 年。
- 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 5 年。

5.5.3 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，确保归档了的文件不会被损坏，防止非授权的访问、修改、删除或其它的篡改行为。

5.5.4 归档文件的备份程序

所有存档文件的数据库除了保存在四川CA的主要存储库，还将在异地保存其备份。

存档的数据库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。

四川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。

5.5.5 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，由操作人员手工记录；对于电子记录，由系统自动增加时间，但这些时间未采用时间戳技术。

5.5.6 归档收集系统

对于系统生成的电子记录，实时同步到日志服务器，进行备份。

对于书面的归档资料，收集归档到文件柜内。

5.5.7 获得和检验归档信息的程序

四川 CA 采取了物理和逻辑的访问控制方法，以确保只有授权人员才能接近这些归档信息，严禁未授权的访问、阅读、修改和删除等操作。

5.6 CA密钥的更替

四川CA的根证书有效期最长不超过25年，任何由其签发的证书，包括CA证书和订户证书，其失效时间不超过根证书的失效时间，任何由 CA 证书签发的订户证书，其失效时间不超过CA证书的失效时间。

CA证书对应的密钥对，当其寿命超过本CPS规定的最大生命期时，四川CA将启动密钥更新流程，替换已经过期的CA密钥对。四川CA密钥变更按如下方式进行：

- 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（“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 或订户证书请求，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。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

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

- 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。

5.7.2 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。

5.7.3 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吊销其证书，或者立即通过电话、电子邮件的方式通知四川 CA 或注册机构吊销其证书。四川 CA 按 4.9 发布证书吊销信

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或注册机构将立即吊销证书，并通知证书订户，订户必须立即停止使用其私钥。四川 CA 按4.9发布证书吊销信息。
- 当四川CA的根CA证书或中级CA证书出现私钥损害时，四川CA将按照密钥应急方案进行紧急处理，并及时通过邮件方式通知依赖方及应用软件供应商。

5.7.4 灾难后的业务存续能力

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措施，能够应对常见的灾难事故，一旦发生灾难，四川 CA 能够根据业务连续性计划恢复业务。

5.8 CA或RA的终止

当四川 CA 及其注册机构需要停止其业务时，将会严格按照《中华人民共和国电子签名法》及相关法规中对认证机构中止业务的规定要求进行有关工作。

6. 技术安全控制

6.1 密钥对的产生和安装

6.1.1 密钥对的产生

6.1.1.1 CA密钥对的产生

四川 CA 的密钥使用国家密码主管部门批准和许可的加密设备生成，该设备对密钥的生成、管理、存储、备份和恢复遵循国家密码主管部门相关规范要求。

CA密钥对的生成过程，由四川CA专门的密钥管理员及多名可信雇员、以及四川CA内部审计人员或独立第三方审计人员见证下，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。

6.1.1.2 订户密钥对的产生

订户密钥对由订户自身的服务器或其它设备内置的密钥生成机制生成。如果订户申请时提交的是一个包含弱算法的 PKCS#10 申请文件，四川CA会拒绝该申请，并建议用户生成新的密钥对。

四川CA不替订户生成密钥对。

6.1.2 私钥传送给订户

不适用。

6.1.3 公钥传送给证书签发机关

订户或订户通过注册机构，将PKCS#10格式的证书签名请求信息或其他数字签名的文件包，以电子文本的方式将公钥提交给四川 CA 签发证书，当需要通过网络传送时将使用安全套接层协议（SSL）或其他安全加密方式。

6.1.4 CA公钥传送给依赖方

四川CA的公钥包含在四川CA自签发的根 CA 证书和中级 CA 证书中，订户和依赖方可从四川CA官网下载根 CA 证书和中级 CA 证书。

6.1.5 密钥的长度

四川CA的SM2根CA证书使用长度为256位的SM2密钥，签名算法为SM3withSM2；

中级 CA 证书使用长度为 256 位的 SM2 密钥，签名算法为 SM3withSM2；

订户证书使用长度为 256 位的 SM2 密钥，签名算法为 SM3withSM2；

四川CA将依据国家密码管理局发布的标准进行密钥算法及长度的调整。

6.1.6 公钥参数的生成和质量检查

公钥参数使用获得国家密码管理局许可资质的加密设备和硬件介质生成，并遵从这些设备的生成规范和标准。

对于参数质量的检查，由于使用获得国家密码管理局许可资质的加密设备和硬件介质生成和存储密钥，已经具备足够的安全等级要求。

6.1.7 密钥使用目的

四川 CA 签发的 X.509v3 证书包含了密钥用法扩展项，其用法与 RFC5280 标准相符。在证书的密钥用法扩展项中指明了用途，证书订户必须按照该指明的用途使用密钥。

根 CA 密钥一般用于签发以下证书和 CRL：

1)代表根 CA 的自签名证书；

2)中级 CA 的证书、交叉证书；

3)根 CA 和中级 CA 的 CRL（ARL）。

4)特定用途的 PKI 体系功能证书（如 OCSP 证书）；

中级 CA 密钥一般用于签发以下证书和 CRL：

1)订户证书；

2)特定用途的 PKI 体系功能证书（如 OCSP 证书）；

3)订户 CRL。

订户的签名密钥可用于提供身份认证、抗抵赖、以及信息完整性等目的，加密密钥可用于信息加密和解密。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块的标准和控制

四川 CA 的密钥使用国家密码主管部门批准和许可的加密设备生成，该设备对密钥的生成、管理、存储、备份和恢复遵循国家对于密码产品管理的相关规定。

CA 密钥对的生成过程，由四川 CA 专门的密钥管理员及若干名可信雇员在四川 CA 屏蔽机房按照四川 CA 密钥生成规程完成。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。

订户证书的密钥使用国家密码管理部门认可的密码模块生成和存储，订户应妥善保护、保管其密码模块，防止其失窃、丢失、损坏及被非授权的使用。

6.2.2 私钥多人控制（m 选 n）

四川 CA 的各类 CA 私钥的生成、备份、恢复、销毁等操作采用多人控制机制，此机制通过加密设备的 5 选 3 分割管理权限实现，即将私钥的管理权限分割保存在 5 张 IC 卡中

（称为秘密分割份额），这5张IC卡由四川CA的5名可信雇员持有（称为秘密分管者），保存在四川 CA 屏蔽机房内的保险柜中。当需要使用管理员权限时，需选择至少其中 3 名秘密分管者在场并许可的情况下，插入管理员IC卡并输入PIN码，才能对私钥进行生成、备份、恢复、销毁等操作；同样地，加密设备的数据备份 IC 卡也设置为 5 张，密钥备份时采用 5 张 IC 卡存放数据备份秘密分割份额，密钥恢复时采用 5 选 3 多人控制策略控制密钥数据恢复操作。当这些秘密分割份额不使用时，存储在屏蔽机房的保险柜中。

四川 CA 的 CA 私钥的激活需要由密钥管理员持有的操作员 IC 卡。操作员 IC 卡保存在四川 CA 屏蔽机房的保险柜中，直到要激活 CA 私钥时才使用。

6.2.3 私钥托管

四川 CA 所有 CA（包括根 CA 和中间 CA）的私钥不允许托管。

根据国家密码管理部门的要求仅对订户加密证书的私钥进行托管，对签名证书的私钥不提供托管服务。

6.2.4 私钥备份

四川 CA 对根私钥和中间 CA 私钥进行备份，可分为两种，一是按照加密设备制造商提供的操作规范生成数据备份密文文件和数据备份恢复权限 IC 卡并保存到屏蔽机房的保险柜；二是按照加密设备制造商提供的操作规范生成克隆设备和管理员操作员 IC 卡并存放在屏蔽机房中。

对于订户证书，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。

6.2.5 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 5 年。归档 CA 密钥对保存在 6.2.1 所述的硬件密码模块中。

四川 CA 或其注册机构不对订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。

6.2.6 私钥导入、导出密码模块

四川CA的CA密钥对在硬件密码模块上生成、保存和使用。此外，为了实现恢复，四川CA按照加密设备制造商提供的操作规范对CA密钥进行备份。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。

对于订户证书，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 要求订户对导出、导入的私钥必须使用足够安全的口令进行保护，且订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。

6.2.7 私钥在密码模块的存储

四川 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硬件密码模块中，且私钥的使用也在硬件密码模块中进行。

对于订户证书，订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订户其可控制的范围内，订户需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。

6.2.8 激活私钥的方法

四川CA的CA私钥存放在硬件密码模块中，激活需要按本CPS第6.2.2节使用加密设备的操作员权限实现。当需要使用 CA 私钥时（在线或离线），需要密钥管理员提供操作员 IC卡才能完成。

保存在密码模块中的订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）后才能被激活和使用。

6.2.9 解除私钥激活状态的方法

对于四川CA的CA私钥，当CA系统向密码模块发出退出登录或密码管理软件向密码模块发出关闭指令，或存放私钥的硬件密码模块断电,，私钥进入非激活状态。

订户解除私钥激活状态由其自行决定，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。

6.2.10 销毁私钥的方法

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硬件密码模块中，并进行归档，其他的CA私钥备份被安全销毁。同时，所有用于激活私钥的PIN码、IC卡等也必须被销毁。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私钥从硬件密码模块中彻底删除，不留有任何残余信息。

对于订户证书私钥，若不再使用，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授权使用。若私钥对应的公钥证书被吊销、到期作废后，还需要用于信息解密的，订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。

6.2.11 密码模块的评估

四川 CA 使用国家密码管理局批准和许可的密码产品，密码模块的评估由国家密码管理局负责。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

四川 CA 对证书公钥进行归档，证书存放在数据库中并进行异地备份，归档数据定期进行完整性校验。

6.3.2 证书操作期和密钥对使用期限

CA证书的最长有效期不超过25年，订户SSL证书的有效期最长为398天。

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。

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。

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密，私钥的使用期限可以在证书的有效期限以外。

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

6.4 激活数据

6.4.1 激活数据的产生和安装

四川CA的CA私钥的激活数据按照加密设备制造商提供的操作规范，由加密设备产生。

如果订户证书私钥的激活数据是口令，这些口令必须：

- 至少8位字符或数字；
- 至少包含一个字符和一个数字；
- 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。

6.4.2 激活数据的保护

对于 CA 私钥的激活数据，四川 CA 按照可靠的方式由可信人员掌握，存储在四川 CA 屏蔽机房中。

订户的激活数据必须在安全可靠的环境下产生，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窃取。

6.4.3 激活数据的其他方面

存有四川CA的CA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的屏蔽机房内，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两名可信人员的监督下进行。

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。

对于申请证书的订户激活数据的生命周期，建议如下：

1、订户用于申请证书的口令，申请成功后失效。

2、用于保护私钥或者 IC 卡、USBKey 的口令，建议订户根据业务应用的需要随时予以变更，使用期限超过3个月后应要进行修改。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

四川CA的CA系统信息安全管理，按照国标《证书认证系统密码及其相关安全技术规范》、工业和信息化部公布的《电子认证服务管理办法》，参照 ISO27001 信息安全管理体系要求，以及其他相关的信息安全标准，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、逻辑访问控制、网络访问控制等。

对每位拥有系统（包括CA系统、RA系统）业务操作权限的可信人员实行严格的双因素验证机制，登录时采用插入数字证书USBKEY硬件介质及输入PIN码的双因素方式。

对系统运维人员，通过堡垒机登录系统实施操作，确保 CA 软件和数据文件安全可信，不会受到未经授权的访问。

生产系统与其他系统逻辑隔离，可以阻止除指定的应用程序外对生产系统网络的访问。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。只有 CA 系统操作与管理组中的、有必要工作需要、访问系统的可信人员可以通过口令访问 CA 数据库。

6.5.2 计算机安全评估

四川CA的CA系统及其运营环境通过了国家密码管理局和工信部的审查，获得了相应资质。

6.6 生命周期技术控制

6.6.1 系统开发控制

四川CA的CA软件是从具备资质的中国商业CA软件提供商购买。四川CA通过内部变更控制流程来控制证书认证系统的上线工作，并要求运维人员严格按照审批和上线流程执行，以保证系统的安全性和可用性。

6.6.2 安全管理控制

四川CA已制定了各种安全策略、管理制度与流程对认证系统进行安全管理。

认证系统的信息安全管理，严格遵循国家密码管理局的有关运行管理规范进行操作。

认证系统的使用具有严格的控制措施，所有的系统都经过严格的测试验证后才进行安全和使用，任何修改和升级会记录在案。

四川 CA 定期对系统进行安全检查，用来识别设备是否被入侵，是否存在安全漏洞等。

6.6.3 生命期的安全控制

四川 CA 认证系统的软硬件设备具备可持续性的升级计划，其中包括了对软、硬件生命周期的安排。

四川 CA 认证系统使用的算法和密码设备均符合相关标准，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。在 CA 系统运行期间，周期性开展漏洞扫描及渗透测试，并及时消除系统安全弱点。

6.7 网络的安全控制

四川 CA 证书认证系统采用多级防火墙和网络资源安全控制系统的保护，并实施完善的访问控制技术。

为了确保网络安全，证书认证系统安装部署了防火墙、入侵检测、安全审计、病毒防范系统，并且及时更新防火墙、入侵监测、安全审计、病毒防范系统的版本，以尽可能的降低来自于网络的风险。

6.8 时间戳

时间戳系统提供的时间戳服务在技术实现上严格遵循国际标准时间戳协议（RFC3161）,采用标准的时间戳请求、时间戳应答以及时间戳编码格式，时间源采用国家授时中心提供的标准时间。

7. 证书、CRL 和 OCSP

7.1 证书

四川 CA 签发的证书符合国家相关标准的要求，并遵循 RFC 5280 标准。

证书结构的基本域内容参考如下表格。

证书结构的基本域

域	值或值的限制
版本	X.509 版本号 V3
序列号	通过 CSPRNG 生成长度为至少 64 位的非序列性的唯一标识符
签名算法	签发证书时使用的签名算法（见本 CPS 7.1.3 节）
签发者 DN	签发者的甄别名。包含 CN、OU、O、C
有效起始日期	证书的生效日期和时间，使用 UTC/GMT+08:00
有效终止日期	证书的失效日期和时间，使用 UTC/GMT+08:00； 有效期的设置符合本 CPS 规定的限制
主题 DN	证书持有者或实体的甄别名（见本 CPS 7.1.4 节） CA 根证书甄别名，包含：CN(commonName)、OU(organizationUnitName)、O(organizationName)、C(countryName)； CA 中级证书甄别名，包含：CN、OU、O、C；

	订户DV SSL证书甄别名，包含：CN； 订户IV SSL证书甄别名，包含：CN、G(GIVENNAME名)、SN(SURNAME姓)、L(localityName)、S(ST,stateOrProvinceName)、C； 订户OV SSL证书甄别名，包含：CN、OU、O、L、S、C； 订户EV SSL证书甄别名，包含：CN、OU、O、STREET(公司详细街道地址)、POSTALCODE(公司地址邮政编码)、L、S、C、SERIALNUMBER(序列号/营业执照号码)、BUSINESSCATEGORY(业务类别,OID: 2.5.4.15)、jurisdictionlocalityName(公司注册地/辖区名称,OID:1.3.6.1.4.1.311.60.2.1.1)、jurisdictionStateOrProvinceName(注册州/省、管辖州或省名称,OID:1.3.6.1.4.1.311.60.2.1.2)、jurisdictionCountryName(注册国家/地区、管辖国家/地区名称,OID:1.3.6.1.4.1.311.60.2.1.3)。
公钥	使用本CPS 7.1.3节中指定的算法，密钥长度满足 本CPS 6.1.5节指定的要求

7.1.1 版本号

X.509 v3证书。

7.1.2 证书扩展项

四川CA颁发证书的内容和扩展项参考如下表格：

域	根证书	中级证书	订户SSL证书
版本	X.509 版本号 V3	X.509 版本号 V3	X.509 版本号 V3
签名算法	SM3withSM2	SM3withSM2	SM3withSM2
密钥长度	256bits SM2	256bits SM2	256bits SM2
颁发机构密钥标识符	用于识别与颁发机构签名私钥相对应的公钥	用于识别与颁发机构签名私钥相对应的公钥	用于识别与颁发机构签名私钥相对应的公钥

主体密钥标识符	用于区分同一主体使用的不同密钥	用于区分同一主体使用的不同密钥	用于区分同一主体使用的不同密钥
授权信息访问	无	包含了颁发者的 OCSP 响应地址。(accessMethod =1.3.6.1.5.5.7.48.1) 包含了颁发者证书的访问地址。(accessMethod =1.3.6.1.5.5.7.48.2)	包含了颁发者的 OCSP 响应地址。(accessMethod =1.3.6.1.5.5.7.48.1) 包含了颁发者证书的访问地址。(accessMethod =1.3.6.1.5.5.7.48.2)
CRL 分发点	无	由四川 CA 指定的 CRL 发布点扩展项，依赖方可根据该扩展项提供的地址和协议下载 CRL	由四川 CA 指定的 CRL 发布点扩展项，依赖方可根据该扩展项提供的地址和协议下载 CRL
主体备用名	无	无	包含一个或多个可选替换名（可使用多种名称形式中的任一个）供实体使用
证书策略	无	包含了颁发者 CA 的 CPS 发布地址	包含颁发者指定的 policy Identifier 或 CA/Browser 论坛中保留的 policy Identifier。包含了颁发者 CA 的 CPS 发布地址
增强密钥算法	无	服务器身份验证(1.3.6.1.5.5.7.3.1)	服务器身份验证(1.3.6.1.5.5.7.3.1)

		客户端身份验证(1.3.6.1.5.5.7.3.2)	客户端身份验证(1.3.6.1.5.5.7.3.2)
基本约束	CA 证书的基本限制扩展项中的主体类型被设为 CA	CA 证书的基本限制扩展项中的主体类型被设为 CA	订户证书的基本限制扩展项的主体类型设为最终实体 (End-Entity)
密钥用法	指明已认证的公开密钥用于何种用途。	指明已认证的公开密钥用于何种用途。	指明已认证的公开密钥用于何种用途。

7.1.2.1密钥用法（Key Usage）

该扩展项指定证书密钥对的用法，包括：数字签名、不可抵赖、密钥加密、数据加密、密钥协议，证书签名，CRL 签名，只加密，只解密，只签名。

CA证书密钥用法：Certificate Signing, Off-line CRL Signing, CRL Signing;

订户签名证书密钥用法：Digital Signature, Non-Repudiation;

订户加密证书密钥用法：Key Encipherment, Data Encipherment, Key Agreement;

7.1.2.2证书策略扩展项（Certificate Policies）

证书策略扩展项中有四川CA对应证书类的 CP 对象标识符及策略限定符。

7.1.2.3主体备用名（subjectAltName）

主题备用名称包含一个或多个可选替换名（可使用多种名称形式中的任一个）供实体使用，CA 把该实体与认证的公开密钥绑定在一起。处于该域中的任何信息必须全部经过审核。

7.1.2.4基本限制扩展项（BasicConstraints）

四川CA的CA证书的基本限制扩展项中的主体类型被设为CA。订户证书的基本限制扩展项的主体类型设为最终实体(End-Entity)。

7.1.2.5扩展的密钥用法（Extended Key Usage）

扩展密钥用法指公钥可用于一种或多种用途，作为对密钥用法扩展项中指明的基本用途的补充或替代。

对于SSL证书，Extended Key Usage包括：服务器身份验证（1.3.6.1.5.5.7.3.1)、客户端身份验证（1.3.6.1.5.5.7.3.2)。

7.1.2.6CRL的分发点（cRLDistributionPoints）

四川CA签发的证书中包含CRL的分发点扩展项，依赖方可根据该扩展项提供地址和协议下载CRL。

7.1.2.7颁发机构密钥标识符（authority Key Identifier）

四川CA签发的订户证书及CA证书中包含颁发机构密钥标识符扩展项，此扩展项用于识别与颁发机构签名私钥相对应的公钥，可辨别同一颁发机构使用的不同密钥(由160位的颁发机构证书的公钥进行SHA-1散列运算后的值构成)。

7.1.2.8主体密钥标识符（subject Key Identifier）

订户证书中包含主题密钥标识符扩展项，它标识了被认证的公钥，可用于区分同一主体使用的不同密钥，该值由主体证书的公钥产生（由160位的主体证书的公钥进行SHA-1散列运算后的值构成）。

7.1.3 密钥算法对象标识符

四川CA签发的证书中，密码算法为SM3withSM2，标识符为1.2.156.10197.1.501。

7.1.4 名称形式

四川CA签发的证书名称形式的格式和内容符合X.500的甄别名格式。

7.1.5 名称限制

无规定。

7.1.6 证书策略对象标识符

当使用证书策略扩展项时，证书中包含证书策略的对象标识符，该对象标识符与相应的证书类别对应，证书策略对象标识符同本CPS第1.2节。

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 CRL

四川CA认证系统定期签发CRL，供订户和依赖方查询使用。签发的CRL符合RFC5280标准。

7.2.1 版本号

X.509 V2。

7.2.2 CRL 和CRL条目扩展项

与ITU X.509和RFC5280规定一致。

（1）CRL的版本号：用来指定CRL的版本信息，四川CA采用的是和证书X.509 V3对应的CRL X.509 V2版本。

（2）签名算法：四川CA采用SM3withSM2签名算法。

（3）颁发者：指定签发机构的DN名。

（4）生效时间：指定一个日期/时间值，用以表明本CRL发布的时间。

（5）更新时间：指定一个日期/时间值，用以表明下一次CRL将要发布的时间（本标准强制使用该域）。

（6）吊销证书列表：指定已经吊销的证书列表。本列表中含有证书的序列号和证书被吊销的日期和时间。

（7）CRL 扩展（CRL Extension）：

- 颁发机构密钥标识符(AuthorityKeyIdentifier)：本项标识用来验证在CRL上签名的公开密钥。它能辨别同一CA使用的不同密钥。
- CRL号（CRL Number）。

7.3 OCSP

四川 CA 认证系统提供 OCSP 服务，签发的 OCSP 响应符合 RFC6960 标准，该标准定义了一种标准的请求和响应信息格式以确认证书状态。

7.3.1 版本号

RFC6960 定义的 OCSP V1 版本。

7.3.2 OCSP 扩展项

不使用 OCSP 扩展项。

8. 认证机构审计和其他评估

四川 CA 通过对人事管理、机房物理安全、运营管理安全等方面执行情况的审查、评估，以确定实际发生情况是否与预定的标准、要求一致，称为一致性审计。

8.1 评估的频率和情形

审计是为了检查、确认四川 CA 以及其注册机构是否依据《中华人民共和国电子签名法》、《证书策略》、《电子认证业务规则》以及各项管理制度和安全策略开展业务，发现并纠正不合规操作，以达到规避经营风险、提高服务质量、保障用户权益的目的。

审计分为外部审计与内部审计，内部审计指内部运营审计。外部审计是由法律规定的主管部门、主管部门委托的第三方机构四川 CA 对电子认证服务业务进行审计与评估。外部审计的频率和情形由主管部门确定。

内部审计的频率：每两个月由审计人员进行一次内部运营审计。

8.2 评估者的资质

四川 CA 的内部运营审计由本 CA 机构安全策略委员会任命的审计员实施。被任命的审计员是本 CA 机构的正式雇员。

外部审计的审计人员身份与资格由主管部门决定。四川 CA 对主管部门的审计予以积极配合。

8.3 评估者与被评估者之间的关系

四川CA机构的审计员为机构的正式雇员，且与四川CA的系统管理员、业务管理员、业务操作员的工作岗位不重叠。

主管部门选择的评估者与四川CA不存在任何的商业利益关系。

8.4 评估的内容

审计所涵盖的内容包括：四川CA颁布的CP/CPS/各项涉及电子认证服务的管理制度、规范、办法中关于人事管理、机房物理安全管理、运营管理安全管理、密钥安全以及操作管理、网络安全管理、证书生命周期管理、客户服务的要求。

8.5 对问题与不足采取的措施

针对审计中发现的不合规情况，审计人员负责监督责任部门完成整改并将结果上报安全策略委员会。

原则上从完成审计到整改完成不超过30天，如问题整改确实30天内无法完成的，由审计人员向安全策略委员会报告。

8.6 评估结果的传达与发布

四川 CA 的内部审计结果向安全策略委员会以及审计涉及的注册机构进行通报。除非法律明确要求，审计结果一般不予公开。

外部审计结果是否公开、如何公开由主管部门决定。

9. 其他业务和法律事务

9.1 费用

9.1.1 证书签发和更新费用

四川 CA 可根据提供的电子认证相关服务向本机构的证书订户收取费用，具体收费标准根据市场和管理部门的规定自行决定。四川 CA 在不高于收费标准的前提下有权根据市场情况，对证书价格进行适当调整，并针对不同订户群体推出不同的收费策略或优惠措施。在订户向四川 CA 订购证书时，四川CA将提前告知证书的签发与更新费用。

如果四川CA签署的协议中指明的价格和四川CA公布的价格不一致，以协议中的价格为准。

9.1.2 证书查询的费用

在证书有效期内，四川CA不对证书查询收取专门的费用，但是四川CA保留对此项服务收费的权利。如果用户提出特殊需求，可能需要支付额外的费用，将由四川 CA 与用户协商收取。

9.1.3 证书吊销或状态信息的查询费用

四川CA对吊销列表（CRL）的获取不收取费用。

四川CA不对 OCSP 服务收取费用。

9.1.4 其他服务费用

如果四川CA向订户提供证书存储介质及相关服务，四川CA将在与订户或者其他实体签署的协议中指明该项价格。

9.1.5 退款策略

在实施证书操作和签发证书的过程中，四川 CA 遵守严格的操作程序和策略。除非出现四川CA违背了本 CPS 所规定的责任或其他重大义务的情况，造成订户合同无法履行、订户证书无法使用，四川CA会将相关费用返还给订户，其他情况下，四川CA向订户收取的费用均不退还。

9.2 财务责任

9.2.1 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的原因造成用户在使用证书过程中遭受损失，四川CA将向证书订户、依赖方提供赔偿，四川CA对任何证书订户、依赖方等实体有关证书赔偿的合计责任限制在不超出证书购买价格的10倍。

9.2.2 其他资产

四川 CA 确保本公司拥有足够的财务实力以维持正常运营并保证相应义务的履行，且能够合理承担对订户及依赖方的责任。

9.2.3 对最终实体的保险或担保

如果四川 CA 违反了本 CPS 的规定，证书订户、依赖方等实体可以申请四川 CA 承担赔偿责任（法定或约定免责除外）。在经四川 CA 确认后，可以对该实体进行赔偿，合计赔偿上限不超过本 CPS 9.2.1 保险范围中的规定。

如根据法律规定以及司法判定四川 CA 须承担赔偿和/或补偿责任的，四川 CA 将按照相关法律法规的规定、仲裁机构的裁定或法院的判决承担相应的赔偿责任。

9.3 业务信息保密

9.3.1 保密信息范围

在四川 CA 提供的电子认证服务中，以下信息视为保密信息：

1）审计记录包括：本地日志、服务器日志、归档日志的信息，这些信息被四川CA 视为保密信息，只有安全审计员和业务管理员可以查看；除法律要求，不可在公司外部发布。

2）其他由四川 CA 和注册机构保存的个人和公司信息应视为保密，除法律要求，不可公布。

9.3.2 不属于保密的信息

四川 CA 将以下信息视为不保密信息：

1） 由四川 CA 发行的证书和 CRL 中的信息。

2） 由四川 CA 支持、CPS 识别的证书策略中的信息。

3） 四川 CA 许可的只有四川 CA 订户方可使用的、在四川 CA 网站公开发布的信息。

4） 其它四川 CA 信息的保密性取决于特殊的数据项和申请。

9.3.3 保护保密信息的责任

四川 CA 有妥善保管与保护本 CPS 9.3.1 中规定的保密信息的责任与义务。

9.4 个人隐私保密

9.4.1 隐私保密方案

四川 CA 尊重证书订户的资料的隐私权，保证完全遵照国家对隐私保护的相关规定及法律。同时，四川CA将确保全体职员严格遵从内部工作相关制度和定。

任何订户选择使用四川CA的证书服务，就表明已经同意接受四川CA的隐私保护制度。

9.4.2 作为隐私处理的信息

除了证书中已经包括的信息以及证书状态信息外，订户提供的其他基本信息将被视为隐私处理。作为隐私处理的信息包括：

1) 订户的联系电话；

2) 订户的通信地址和住址；

3) 订户的银行帐号。

这些信息将只能由四川 CA 使用，非经订户同意或有关法律法规、国家相关部门根据合法的程序要求，四川CA不会任意公开。

9.4.3 不被视为隐私的信息

四川CA 定义包括但不限于以下信息不被视为证书订户的隐私信息：

1) 订户姓名、单位名称等。

2) 订户性别、单位性质等。

3) 订户通信地址的邮政编码。

4) 订户的电子邮箱。

5） 订户要求出现在证书中的信息。

9.4.4 保护隐私的责任

四川CA及注册机构有妥善保管与保护本 CPS 第 9.4.2 节中规定的隐私信息的责任与义务。

9.4.5 使用隐私信息的告知与同意

四川 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。

四川 CA 及其注册机构如需超出约定范围及用途使用证书订户的隐私信息，应事先告知证书订户并获得同意及授权；如未获得同意及授权，四川 CA 不会将订户隐私信息透露给任意第三方。

9.4.6 依法律或行政程序的信息披露

依据法律、行政法规、规章、决定、命令等，由于司法执行或法律授权的行政执行需要，四川 CA 及其注册机构有可能需要将有关信息在订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客户隐私信息。

9.4.7 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。

9.4.8 用户个人信息的保护

四川 CA 严格按照《民法典》、《电子签名法》等相关法律法规保护用户的个人信息，在开展业务过程中遵守合法、正当、必要的原则，明确告知用户收集个人信息的目的、方式和范围，并征得用户书面同意。四川 CA 不会对与电子认证业务无关及非必要的个人信息进行收集。

用户如需查阅自身的个人信息，请用户按四川 CA 官方网站公布的联系方式，联系四川 CA 申请查询。

用户个人信息的删除按照法律法规要求或与用户证书服务协议的约定，四川 CA 有权对证书用户个人信息进行删除。

用户在使用 CA 证书服务过程中，个人信息发生变更的，应及时通过四川 CA 官方网站公布的联系方式提出信息变更申请，由于用户自身原因未及时将变更信息通知四川 CA 的，由此发生的风险由用户自身承担。

9.5 知识产权

1） 四川CA享有并保留对证书及四川CA 提供的全部软件、资料、数据等的著作权、专利申请权等全部知识产权；

2） 四川CA享有由本机构制定并发布的 CP、CPS、技术支持手册、发布的证书和 CRL 等的所有权和知识产权；

3） 四川CA官方网站上公布的一切信息均属于四川CA财产，未经四川CA书面允许，他人不得转载用于商业行为；

4） 四川CA对外运营管理策略和规范属于四川CA财产；

5）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。

9.6 陈述与担保

9.6.1 CA的陈述与担保

四川CA在提供电子认证服务活动过程中对订户的承诺如下：

1）签发给订户的证书符合《中华人民共和国电子签名法》及本 CPS 的要求，四川CA按照法律法规及本 CPS 的要求对所签发的数字证书承担相应的法律责任。

2）四川CA将根据 CPS 的要求验证申请人的身份；

3） 四川CA将向证书订户通报任何已知的，将在本质上影响订户证书的有效性和可靠性事件。

4） 四川CA将根据本CPS的要求及时吊销证书。

5）若四川CA与订户无关联，则四川CA与订户是合法有效且可执行的订户协议双方；若四川CA与订户为同一实体或有关联，则申请人代表已认可使用条款；

6） 针对所有未过期的证书的当前状态信息（有效或已吊销）建立及维护 7x24 小时公开的信息库。

7）四川CA不负责评估证书是否在适当的范围内使用，订户和依赖方依照订户协议和依赖方协议确保证书用于允许使用的目的。

9.6.2 RA的陈述与担保

四川CA的注册机构在参与电子认证服务过程中的承诺如下：

1）遵循本 CPS 和四川 CA 的授权协议以及四川 CA 公布的规范和流程，接受并处理申请者的证书服务请求，并依据授权设置、管理下级证书服务机构。

2）RA 必须遵循四川 CA 制定的服务受理规范、系统运作和管理要求，根据本 CPS、四川 CA 公布的规范，RA 有权决定是否给申请者提供相应的证书服务。

3）按照四川 CA 的要求和规范，确定下属证书服务受理机构的设置方式、管理方式和审核方式，这些方式的确定必须以书面的文件形式公布，涵盖并且不得与四川 CA 公布的相关条款产生冲突、矛盾或者不一致。

4）依据本 CPS 的规定，确保其运营系统处在安全的物理环境中，并具备相应的安全管理和隔离措施。RA 必须能够提供证书服务全部的数据资料及备份，并按照四川 CA 的要求，保证其与下属证书服务机构间的信息传输安全。RA 承诺严格执行为所有证书用户提供隐私保密的义务，并愿意承担因此而带来的法律责任。

5）接受四川 CA 根据本 CPS 和授权协议对 RA 进行管理，包括进行服务资质审核和规范执行检查。

6）承认四川 CA 对所有证书服务申请者的服务请求拥有最终处理权。

7）不得拒绝任何来自四川 CA 的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

8）为订户提供必要的技术咨询，使订户顺利地申请和使用证书。

9.6.3 订户的陈述与担保

订户一旦接受四川 CA 签发的证书，就被视为向四川 CA、注册机构及信赖证书的有关当事人作出以下承诺：

1） 订户在申请证书时，已仔细阅读、知悉并接受四川 CA《数字证书服务协议》和本 CPS。

2） 订户在证书的有效期内使用证书私钥进行数字签名。

3） 订户在申请证书时向注册机构提供的信息、资料及所做的陈述都是真实、完整和准确的，如前述信息、资料或陈述发生任何改变将及时书面通知注册机构。如因订户故意或过失提供虚假、伪造等信息资料或陈述，或已提供的信息资料及陈述改变后未及时书面通知注册机构的，由订户自行承担全部法律责任。

4） 如果存在代理人，那么订户和代理人两者负有连带责任。订户有责任就代理人所作的任何不实陈述与遗漏，通知四川CA或其授权的注册机构。

5） 与订户证书所含公钥相对应的私钥所进行的每一次签名，都是订户自己的签名，并且在进行签名时，证书是有效证书（证书没有过期、吊销），证书的私钥为订户自身访问和使用。

6） 一经接受证书，即表示订户知悉且接受本 CPS 中的所有条款和条件，并知悉和接受相应的《数字证书服务协议》。

7） 一经接受证书，订户就应当承担如下责任：始终保持对其私钥的控制；使用可信的系统；采取安全、合理的预防措施来防止私钥的遗失、泄漏、被篡改或被未经授权使用，如订户知道或者应当知道证书私钥或密码已经或者可能已经遗失、泄漏、被篡改或被未经授权使用的，应及时书面告知有关各方并终止使用证书。

8）不得拒绝任何来自四川CA公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

9） 证书在本 CPS 中规定的使用范围内合法使用，只将证书用于经过授权的或其他合法的使用目的，不将证书用于使用目的以外的场合。

9.6.4 依赖方的陈述与担保

依赖方声明并承诺：

1） 熟悉本CPS的条款，了解证书的使用目的，遵守本CPS的所有规定，同意本 CPS中关于CA机构责任限制的规定；

2）获取并安装该证书对应的证书链，在信赖证书前，对证书的信任链进行验证；

3）在信赖证书所证明的信任关系前确认该证书有效，包括：通过查询CRL或OCSP确认证书是否被撤销；确认证书在规定的范围和期限使用；检查该证书路径中所有出现过的证书的可靠性；确认该证书记载的内容与所要证明的内容一致；检查其他可能影响证书有效性的信息；

4） 不得拒绝任何来自 CA 机构公示过的声明、变更、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等；

5） 依赖方一旦由于疏忽或其他原因违背了合理检查的条款，依赖方应就此给 CA 机构带来的损失进行赔偿，并应承担因此造成的自身或他人损失。

9.6.5 其他参与者的陈述与担保

从事电子认证活动的其他参与者须承诺遵守本 CPS 的所有规定。

9.7 担保免责

除本 CPS 9.6.1 中的明确承诺外，四川 CA 不承担其他任何形式的保证和义务：

1） 不保证证书订户、依赖方、其他参与者的陈述内容；

2） 不对电子认证活动中使用的任何软件做出保证；

3） 不对证书在超出规定目的以外的应用承担任何责任；

4） 不对由于不可抗力，如战争、自然灾害等造成的服务中断并由此造成的客户损失承担责任；

5） 订户违反本 CPS 9.6.3 之承诺时，或依赖方违反本 CPS 9.6.4 之承诺时，四川 CA 免责。

9.8 有限责任

证书订户、依赖方因四川 CA 提供的电子认证服务从事民事活动遭受损失，四川 CA 将承担不超过本 CPS 9.9 规定的有限赔偿责任。

9.9 赔偿

9.9.1 CA 的赔偿责任

四川 CA 只对由于自身原因造成证书订户、依赖方的直接损失承担责任，对间接损失不承担责任。

四川 CA 对于直接损失所负法律责任的上限为：在任何情况下每张证书赔偿额不得超过证书购买价格的 10 倍。每张证书的责任均按该上限而不考虑电子签名和交易处理等有关的其他索赔的数量。当超过赔偿上限时，可用的赔偿上限将首先分配给最早得到索赔解决的一方。四川 CA 没有责任为每张证书支付高出赔偿上限的赔偿金，而不管赔偿上限的总量在索赔提出者之间是如何分配的。

如四川 CA 违反了本 CPS 第 9.6.1 节中的陈述，证书订户、依赖方等最终实体可以申请赔偿（法定或约定免责除外）。如出现下述情形，四川 CA 承担有限赔偿责任：

1） 四川 CA 将证书错误的签发给订户以外的第三方，导致订户或依赖方遭受损失的；

2） 在订户提交信息或资料真实、完整、准确的情况下，四川 CA 签发的证书出现了错误信息，导致订户或依赖方遭受损失的；

3） 在四川 CA 明知订户提交信息或资料存在虚假谎报的情况，但仍然向订户签发证书，导致依赖方遭受损失的；

4） 由于四川 CA 的原因导致证书私钥被破译、窃取、泄漏，导致订户或依赖方遭受损失的；

5） 四川 CA 未能及时吊销证书，导致依赖方遭受损失的。

另外，四川 CA 赔偿限制如下：

1） 四川 CA 所有的赔偿义务不得高于四川 CA 所承担的上限额度，这种赔偿上限可以由四川 CA 根据情况重新制定，四川 CA 会将重新制定后的情况立刻通知相关当事人。

2） 对于由订户或依赖方的原因造成的损失，四川 CA 不承担任何赔偿责任，由订户或依赖方自行承担。

3） 在证书有效期内产生的损失，订户或依赖方应在知道或应当知道损失发生之日起三年内向四川 CA 书面提出索赔；超出三年的，该索赔无效。

9.9.2 订户的赔偿责任

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：

1） 订户申请注册证书时，因故意、过失或者恶意提供不真实、不完整、不准确资料，造成四川 CA 及其授权的注册机构或者第三方遭受损害；

2） 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有及时告知四川 CA 及其注册机构以及不当交付他人使用造成四川 CA 及其注册机构、第三方遭受损害；

3） 订户使用证书的行为，有违反本 CPS 及相关操作规范，或者将证书用于非本 CPS 规定的业务范围；

4） 自证书订户或者其他有权提出吊销证书的实体提出吊销请求，至四川 CA 将该证书吊销信息予以发布期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果四川CA按照本 CPS 的规范进行了有关操作，那么该证书订户必须承担吊销信息发布之前的所有损害赔偿责任；

5） 证书中的信息发生变更但未停止使用证书并及时通知四川CA和依赖方；

6） 没有对私钥采取有效的保护措施，导致私钥丢失或被损害、窃取、泄漏等；

7） 在得知私钥丢失或存在危险时，未停止使用证书并及时通知四川CA和依赖方；

8） 超出证书有效期限使用证书的；

9） 订户的证书信息侵犯了第三方的知识产权；

10） 在规定的范围及目的外使用证书，如从事违法犯罪活动的。

9.9.3 依赖方的赔偿责任

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：

1） 依赖方没有执行四川CA与依赖方的协议或本 CPS 规定的义务，导致四川CA 及注册机构或第三方遭受损害；

2） 未能依照本 CPS 规定对证书进行合理审核，导致四川CA及注册机构或第三方遭受损害；

3） 依赖方没有对证书的信任链进行验证，导致四川 CA 及注册机构或第三方遭受损害；

4） 依赖方没有通过查询 CRL 或 OCSP 确认证书是否被吊销，导致四川CA及注册机构或第三方遭受损害。

5） 在不合理的情形或环境下信赖证书，如依赖方明知证书存在超范围、超期限使用的情形或证书已经或有可能被人窃取的情形，但仍然信赖证书。

9.10 有效期限与终止

9.10.1 有效期限

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

9.10.2 终止

当四川CA终止业务时，四川CA的CPS终止。在终止服务六十日前向电子认证服务主管部门报告，并作出妥善安排。

四川CA的CPS终止（而非更新），则意味着四川CA电子认证业务的终止。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。

9.11 对参与者个别通告与沟通

四川CA及其注册机构在必要的情况下，如在主动吊销订户证书、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、依赖方。

9.12 修订

9.12.1 修订程序

本CPS将尽量避免不必要的修改。但四川CA将不定期地对本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的CPS编写小组将对本CPS及其他相关文档、协议提出修改建议，报四川CA安全策略委员会审核批准，批准后予以正式发布。

9.12.2 通知机制与期限

四川CA将修改后的CPS通过四川CA网站发布，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。

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、或现有CPS有缺陷时，必须修改本CPS。

9.13 争议解决

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友好协商解决，协商解决不了的，当事人因与四川 CA、四川 CA 授权的注册机构在电子认证活动中产生的任何争端及或对本 CPS 所产生的任何争议应向四川 CA 所在地有管辖权的人民法院诉讼解决。

9.14 管辖法律

本 CPS 在各方面服从中华人民共和国法律和法规的管制和解释，包括但不限于《中华人民共和国电子签名法》及《电子认证服务管理办法》等。

9.15 与适用法律的符合性

四川 CA 的所有业务、活动、合同、协议符合中华人民共和国法律、法规，包括但不限于《公司法》《民法典》《消费者权益保护法》等。

9.16 一般条款

9.16.1 完整协议

四川CA与用户协商后另行确定其他条款，包括未在上述说明的其他相关内容条款。

9.16.2 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。

9.16.3 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应该影响协议中其他条款的效力。

9.16.4 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，胜诉方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。

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。在电子认证活动中，四川 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 其他条款

四川CA承诺遵循 CA/Browser Forum(https://www.cabforum.org.)发布的最新版本的《EV 证书指导准则 Guidelines For The Issuance And Management Of Extended Validation Certificates》《公众可信证书签发和管理基线要求 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates》，若CPS与以上两个指导准则不符，以准则为准。