



四川 CA 电子认证业务规则

1.2 版本

版本说明：

四川 CA 电子认证业务规则版本控制表

名称及版本	主要修改说明	发布时间	修改人
四川 CA 电子认证业务规则 1.0	新版本发布	2016 年 4 月	尹才敏
四川 CA 电子认证业务规则 1.1	1、修订“1.5.2/1.5.4/9.12.1”CPS 修订、批准机构和程序； 2、修订“5.4.2 处理日志周期”； 3、修订“6.2.2 私钥多人控制”； 4、版本号和发布时间变更。	2018 年 11 月 9 日	尹才敏 /徐涯
四川 CA 电子认证业务规则 1.2	1、修改、订正文字错误； 2、校正、补充部分章节表述； 3、增加场景证书、注册受理点 (LRA)、测试证书说明； 4、增加机构、个人申请验证方式； 5、“组织机构代码”替换为“统一 社会信用代码”； 6、证书到期前 30 天可更新改为 60 天。	2019 年 4 月 1 日	编写小 组

目 录

1. 概括性描述.....	1
1.1 概述	1
1.2 文档名称与标识	1
1.3 电子认证活动参与者	2
1.3.1 电子认证服务机构 (CA)	2
1.3.2 注册机构 (RA)	2
1.3.3 证书注册受理点 (LRA)	2
1.3.4 订户	3
1.3.5 依赖方	3
1.3.6 其他参与者	3
1.4 证书应用	3
1.4.1 正式证书和测试证书	3
1.4.2 合适的应用	4
1.4.3 受限的应用	4
1.5 策略管理	5
1.5.1 策略文档管理机构	5
1.5.2 联系人	5
1.5.3 决定 CPS 符合策略的机构	5
1.5.4 CPS 批准和修订程序	5
1.6 定义与缩写	6
1.6.1 定义	6
1.6.2 缩写	8
2. 信息发布与管理	9
2.1 信息库	9
2.2 认证信息的发布	9
2.2.1 CPS 的发布	9

2.2.2	证书和 CRL 发布	10
2.3	发布的时间或频率	10
2.3.1	CPS 的发布时间和频率	10
2.3.2	证书发布时间和频率	10
2.3.3	CRL 的发布时间和频率	10
2.4	信息库访问控制	10
3.	身份标识与鉴证	11
3.1	命名	11
3.1.1	名称类型	11
3.1.2	对名称有意义的要求	12
3.1.3	订户的匿名或伪名	13
3.1.4	理解不同名称形式的规则	13
3.1.5	名称的唯一性	13
3.1.6	商标的识别、鉴证和角色	13
3.2	初始身份确认	13
3.2.1	证明拥有私钥的方法	13
3.2.2	机构身份的鉴证	14
3.2.3	个人身份的鉴证	15
3.2.4	场景证书订户身份的鉴证	15
3.2.5	没有验证的订户信息	16
3.2.6	授权的确认	16
3.2.7	互操作准则	16
3.3	密钥更新请求的标识与鉴证	16
3.3.1	常规的密钥更新的标识与鉴证	17
3.3.2	吊销之后的密钥更新的标识与鉴证	17
3.4	吊销请求的标识与鉴证	17
3.4.1	吊销操作	17

3.4.2	吊销申请与确认	17
3.5	授权服务机构的标识与鉴别	18
4.	证书生命周期操作要求	18
4.1	证书申请	18
4.1.1	证书申请实体	18
4.1.2	注册过程与责任	18
4.2	证书申请处理	19
4.2.1	测试证书的申请处理	19
4.2.2	执行识别与鉴别功能	19
4.2.3	证书申请批准和拒绝	19
4.2.4	处理证书申请的时间	20
4.3	证书签发	20
4.3.1	证书签发中 RA 和 CA 的行为	20
4.3.2	CA 和 RA 对订户的通知	20
4.4	证书接受	21
4.4.1	构成接受证书的行为	21
4.4.2	CA 对证书的发布	21
4.4.3	CA 对其他实体的通告	21
4.5	密钥对和证书使用	21
4.5.1	订户私钥和证书使用	22
4.5.2	依赖方公钥和证书使用	22
4.6	证书更新	22
4.6.1	证书更新的情形	22
4.6.2	请求证书更新的实体	23
4.6.3	证书更新请求的处理	23
4.6.4	签发新证书时对订户的通知	24
4.6.5	构成接受更新证书的行为	24

4.6.6	CA 对更新证书的发布	24
4.6.7	CA 对其他实体的通告	24
4.7	证书密钥更新	24
4.7.1	证书密钥更新的情形	24
4.7.2	请求证书密钥更新的实体	25
4.7.3	证书密钥更新请求的处理	25
4.7.4	签发新证书时对订户的通知	25
4.7.5	构成接受密钥更新证书的行为	25
4.7.6	CA 对密钥更新证书的发布	25
4.7.7	CA 对其他实体的通告	26
4.8	证书变更	26
4.8.1	证书变更的情形	26
4.8.2	请求证书变更的实体	26
4.8.3	证书变更请求的处理	26
4.8.4	签发新证书时对订户的通告	26
4.8.5	构成接受变更证书的行为	26
4.8.6	CA 对变更证书的发布	26
4.8.7	CA 对其他实体的通告	26
4.9	证书吊销和挂起	27
4.9.1	证书吊销的情形	27
4.9.2	请求证书吊销的实体	27
4.9.3	吊销请求的流程	27
4.9.4	吊销请求宽限期	28
4.9.5	CA 处理吊销请求的时限	28
4.9.6	依赖方检查证书吊销的要求	28
4.9.7	CRL 发布频率	29
4.9.8	CRL 发布的最大滞后时间	29
4.9.9	在线状态查询的可用性	29

4.9.10	在线状态查询要求	29
4.9.11	吊销信息的其他发布形式	29
4.9.12	密钥损害的特别要求	29
4.9.13	证书挂起的情形	29
4.10	证书状态服务	29
4.10.1	操作特征	30
4.10.2	服务可用性	30
4.10.3	可选特征	30
4.11	订购结束	30
4.12	密钥托管与恢复	31
4.12.1	密钥托管与恢复的策略与行为	31
4.12.2	会话密钥的封装与恢复的策略与行为	31
5.	认证机构设施、管理和操作控制.....	31
5.1	物理控制	31
5.1.1	场地位置与建筑	31
5.1.2	物理访问控制	32
5.1.3	电力与空调	32
5.1.4	水患防治	32
5.1.5	火灾防护	33
5.1.6	介质存储	33
5.1.7	废物处理	33
5.1.8	异地备份	33
5.1.9	注册机构物理控制	34
5.2	程序控制	34
5.2.1	可信角色	34
5.2.2	每项任务需要的人数	34
5.2.3	每个角色的识别与鉴别	35

5.2.4	需要职责分割的角色	35
5.3	人员控制	35
5.3.1	资格、经历和无过失要求	35
5.3.2	背景审查程序	36
5.3.3	培训要求	36
5.3.4	再培训周期和要求	37
5.3.5	工作岗位轮换周期和顺序	37
5.3.6	未授权行为的处罚	37
5.3.7	独立合约人的要求	37
5.3.8	提供给员工的文档	37
5.4	审计日志程序	37
5.4.1	记录事件的类型	37
5.4.2	处理日志的周期	39
5.4.3	审计日志保存期限	39
5.4.4	审计日志的保护	39
5.4.5	审计日志备份程序	39
5.4.6	审计收集系统	39
5.4.7	对导致事件主体的通知	39
5.4.8	脆弱性评估	39
5.5	记录归档	40
5.5.1	归档记录的类型	40
5.5.2	归档记录的保存期限	40
5.5.3	归档文件的保护	40
5.5.4	归档文件的备份程序	40
5.5.5	记录时间戳要求	41
5.5.6	归档收集系统	41
5.5.7	获得和检验归档信息的程序	41
5.6	CA 密钥变更	41

5.7	损害与灾难恢复	41
5.7.1	事故和损害处理程序	41
5.7.2	计算机资源、软件和/或数据的损坏	42
5.7.3	实体私钥损害处理程序	42
5.7.4	灾难后的业务存续能力	42
5.8	CA 或 RA 的终止	42
6.	技术安全控制	43
6.1	密钥对的产生和安装	43
6.1.1	密钥对的产生	43
6.1.2	私钥传送给订户	43
6.1.3	公钥传送给证书签发机关	44
6.1.4	CA 公钥传送给依赖方	44
6.1.5	密钥的长度	44
6.1.6	公钥参数的生成和质量检查	44
6.1.7	密钥使用目的	45
6.2	私钥保护和密码模块工程控制	45
6.2.1	密码模块的标准和控制	45
6.2.2	私钥多人控制	46
6.2.3	私钥托管	46
6.2.4	私钥备份	46
6.2.5	私钥归档	46
6.2.6	私钥导入、导出密码模块	47
6.2.7	私钥在密码模块的存储	47
6.2.8	激活私钥的方法	48
6.2.9	解除私钥激活状态的方法	48
6.2.10	销毁私钥的方法	49
6.2.11	密码模块的评估	49

6.3	密钥对管理的其他方面	49
6.3.1	公钥归档	49
6.3.2	证书操作期和密钥对使用期限	49
6.4	激活数据	50
6.4.1	激活数据的产生和安装	50
6.4.2	激活数据的保护	50
6.4.3	激活数据的其他方面	51
6.5	计算机安全控制	52
6.5.1	特别的计算机安全技术要求	52
6.5.2	计算机安全评估	52
6.6	生命周期技术控制	52
6.6.1	系统开发控制	52
6.6.2	安全管理控制	52
6.6.3	生命期的安全控制	52
6.7	网络的安全控制	53
6.8	时间戳	53
7.	证书、CRL 和 OCSP	53
7.1	证书	53
7.1.1	版本号	54
7.1.2	证书扩展项	54
7.1.3	密钥算法对象标识符	55
7.1.4	名称形式	56
7.1.5	名称限制	56
7.1.6	证书策略对象标识符	56
7.1.7	策略限制扩展项的用法	56
7.1.8	策略限定符的语法和语义	56
7.1.9	关键证书策略扩展项的处理规则	56

7.2	CRL	56
7.2.1	版本号	57
7.2.2	CRL 和 CRL 条目扩展项	57
7.3	OCSP	57
7.3.1	版本号	57
7.3.2	OCSP 扩展项	58
8.	认证机构审计和其他评估	58
8.1	评估的频率和情形	58
8.2	评估者的资质	58
8.3	评估者与被评估者之间的关系	59
8.4	评估的内容	59
8.5	对问题与不足采取的措施	59
8.6	评估结果的传达与发布	59
8.7	其他评估	59
9.	其他业务和法律事务	60
9.1	费用	60
9.1.1	证书签发和更新费用	60
9.1.2	证书查询的费用	60
9.1.3	证书吊销或状态信息的查询费用	60
9.1.4	其他服务费用	60
9.1.5	退款策略	60
9.2	财务责任	60
9.2.1	保险范围	60
9.2.2	其他资产	61
9.2.3	对最终实体的保险或担保	61
9.3	业务信息保密	61
9.3.1	保密信息范围	61

9.3.2	不属于保密的信息	61
9.3.3	保护保密信息的信息	62
9.4	个人隐私保密	62
9.4.1	隐私保密方案	62
9.4.2	作为隐私处理的信息	62
9.4.3	不被视为隐私的信息	62
9.4.4	保护隐私的责任	62
9.4.5	使用隐私信息的告知与同意	62
9.4.6	依法律或行政程序的信息披露	63
9.4.7	其他信息披露情形	63
9.5	知识产权	63
9.5.1	证书和吊销信息中的知识产权	63
9.5.2	CPS 中的知识产权	63
9.5.3	命名中的知识产权	63
9.5.4	密钥和密钥材料的知识产权	63
9.6	陈述与担保	63
9.6.1	CA 的陈述与担保	63
9.6.2	RA 的陈述与担保	64
9.6.3	订户的陈述与担保	64
9.6.4	依赖方的陈述与担保	65
9.6.5	其他参与者的陈述与担保	65
9.7	担保免责	65
9.8	有限责任	65
9.9	赔偿	66
9.10	有效期限与终止	67
9.10.1	有效期限	67
9.10.2	终止	67
9.10.3	效力的终止与保留	67

9.11	对参与者个别通告与沟通	67
9.12	修订	67
9.12.1	修订程序	67
9.12.2	通知机制与期限	68
9.12.3	必须修改业务规则的情形	68
9.13	争议解决	68
9.14	管辖法律	68
9.15	与适用法律的符合性	68
9.16	一般条款	68
9.16.1	完整协议	68
9.16.2	转让	69
9.16.3	分割性	69
9.16.4	强制执行	69
9.16.5	不可抗力	69
9.17	其他条款	69

1. 概括性描述

四川省数字证书认证管理中心有限公司（简称四川 CA），是全省统一数字认证体系的重要组成部分，是四川省信息安全的重要基础设施，具备提供符合《中华人民共和国电子签名法》规定的数字证书和电子认证服务的能力。

作为国内专注于电子认证服务的运营商，四川 CA 依靠先进而实用的技术和优质的服务，为广大的、对通信和信息安全方面有各种各样需求的公众用户提供数字证书认证服务。

本文档《四川 CA 电子认证业务规则》（Certification Practice Statement, CPS），阐明了四川 CA 如何开展认证业务，包括批准、签发、管理、吊销和更新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。

本 CPS 的总体条款结构符合信息产业主管部门所发布的《电子认证业务规则规范（试行）》，并在制定过程中参照《中华人民共和国电子签名法》、《电子认证服务管理办法》、及国家密码主管部门相关标准制定。在不改变《电子认证业务规则规范（试行）》总体框架的情况下，在制定本 CPS 时可能会对该框架进行扩充，以适应四川 CA 认证业务的特定需求。

本 CPS（v1.2 版本）的生效日期是 2019 年 4 月 1 日。

1.1 概述

本 CPS 适用于四川 CA 运营管理的认证体系 CA，包括四川 CA 根 CA、根 CA 之下的证书签发 CA、以及为机构用户创建并运营的子 CA。用户的子 CA 托管在四川 CA、由四川 CA 负责运营。机构用户在其子 CA 下签发证书时，必须遵从本 CPS 开展认证业务。

1.2 文档名称与标识

本文档称为《四川省数字证书认证管理中心有限公司电子认证业务规则》（简称四川 CA CPS）。

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，向订户颁发包括机构证书、个人证书、设备证书在内的各类公钥证书。

与四川 CA 建立起合同关系的第三方机构客户，可作为四川 CA 认证体系下的一个下级认证机构，拥有子 CA 并开展其认证业务，但其子 CA 托管在四川 CA，由四川 CA 负责维护和运营。

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，同时也承担部分 RA 的角色，也可以授权建立外部 RA。各类政府机构、企事业单位以及社会团体等各类组织机构等均可以申请成为四川 CA 认证服务体系架构内的注册机构。外部 RA 须经四川 CA 评估及审批，方可授权其作为注册机构。

各 RA 应遵循本 CPS 以及四川 CA 与之签署的授权协议。需要特别指出的是，外部 RA 不拥有四川 CA 的设备证书相关服务操作权限，包括但不限于申请设备证书的信息验证和证书签发等操作权限。

1.3.3 证书注册受理点（LRA）

证书注册受理点是面向订户的最终服务机构，经过四川 CA 或其授权单位的审查，可以授权某特定单位或实体成为证书注册受理点，负责向 RA 提供申请实体的信息，包括申请实体的名称、可以表明身份的法定标识以及四川 CA 要求的其他合法的证明文件、联系信息等，并根据这些信息为申请实体提供证书申请、证书制作、签名密钥生成、证书查询、证书吊销、证书更新等被授权的服务或技术支持。

受理点必须遵照本 CPS 以及四川 CA 与之签署的授权协议开展服务工作。

1.3.4 订户

“订户”指从四川 CA 获得证书的个人、组织机构，即最终用户（end-user）。订户通常需要同四川 CA 注册机构，或其授权机构签订合约获得证书，并承担作为证书订户的责任。

“主体”（subject）特指证书标识的实体，或者被签发证书的实体，也即证书中主体名字段（Subject Name）所标识的实体。

在有些情况下，证书订户和证书主体是同一个实体，如个人证书、机构证书；但在有些情况下，证书订户和主体不是同一实体，如设备证书的订户是设备所属机构，而证书主体是设备。

证书申请者指正在申请证书的证书订户或其授权者。在有些情况下，证书申请者和证书订户是同一个实体，如个人证书；但在有些情况下，他们是不同的实体，如机构证书的订户是该组织机构，而申请者是往往其授权人。再比如，一个组织可能为其雇员请求证书，其雇员是真正的证书订户（需要承担订户的责任），而组织机构是其授权申请者。

证书持有者即证书订户或最终用户。

1.3.5 依赖方

四川 CA 信任域的依赖方是为某一应用而使用、信任四川 CA 或其注册机构签发的证书的个人或机构。依赖方可以是四川 CA 的证书订户，也可以不是订户。

1.3.6 其他参与者

其他参与者指为四川 CA 证书服务体系提供相关服务的其他实体。

1.4 证书应用

1.4.1 正式证书和测试证书

四川 CA 认证服务体系中支持正式证书和测试证书。

正式证书的申请者必须遵照四川 CA 证书申请流程并通过四川 CA 需要的鉴别程序，除场景证书外，证书有效期一般为 1 年。

测试证书申请者可通过离线、在线方式向四川 CA 申请，有效期不超过 12 个月。测试证书仅用于系统测试的使用，不能作为任何数字证书正式用途的使用。

1.4.2 合适的应用

1.4.2.1 机构证书

机构证书颁发对象可以是企业、政府机关事业单位、以及社会团体等各类组织机构；可用于需要区分、标识、鉴别机构身份的场合，还可用于数据加解密和信息签名，包括订单、合同签名，以实现信息保密，提供信息源发性证明、完整性保障和抗抵赖。

1.4.2.2 个人证书

个人证书，包括企业个人（如招投标代表）、企业法定代表人、公务人员，也可以是独立自然人，可用于需要区分、标识、鉴别个人身份的场合，还可用于数据加解密和信息签名，包括订单签名，以实现信息保密，提供信息源发性证明、完整性保障和抗抵赖。

1.4.2.3 场景证书

适用于对即时业务或者特定场景业务进行单次数字签名的数字证书，用于对当事人及行为数据摘要进行固化。使用场景证书对即时业务或者场景业务证据签名后可证明证据在产生、结束后无篡改，并保证多个证据之间的关联性和一致性。

场景证书所对应的私钥为一次性使用，其在使用一次后即被销毁。

1.4.2.4 设备证书

设备证书用于标识服务器、运营设备，还可用于数据加解密和信息签名，以实现信息保密，及提供信息源发性证明、完整性保障。

证书申请人根据实际需要，决定采用哪种证书类型。

1.4.3 受限的应用

证书禁止在任何违反国家法律、法规或破坏国家安全的情形下使用，否则由此造成的法律后果由用户自己承担。

四川 CA 所颁发的某些证书在功能上是受到限制的，如个人证书只能用于个人订户的应用，而不能作为服务器证书或机构证书使用。机构证书只能用于代表组织机构的场合。

证书的密钥用法扩展项中限制了与证书中公钥对应私钥的使用目的，如最终用户证书不能作为 CA 证书使用。这种限制是由基本限制扩展项缺省值确定的。然而，基于扩展项的限制的有效性取决于软件，如果有关软件不遵守有关约定，其对证书的使用将超出本 CPS 限定的应用范围，将是不受保护的。

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《电子认证业务规则》的制定、发布、更新等事宜。

本《电子认证业务规则》由四川省数字证书认证管理中心有限公司拥有完全版权。

1.5.2 联系人

本《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

邮编：610041

电话：028-85336171 传真：028-85336171-808

1.5.3 决定 CPS 符合策略的机构

本《电子认证业务规则》由四川 CA CPS 编写小组负责组织制定、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

《四川 CA 电子认证业务规则》（CPS）由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成立 CPS 编写小组，编写小组负责修订，并向安全策略委员会提交修订内容，由安全策略委员会批准通过。通过后在公司网站发布修订版《四川 CA 电子认证业务规则》，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
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。
证书链	一个有序的证书列表，包含了最终用户的证书和发证机关的证书，该列表最顶级证书为根证书，最下级证书为最终用户的证书。
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。
挑战语	证书申请者在注册一个证书时选择的秘密短语。当一个证书被签发后，证书申请者成为了一个订户，这时如果订户要求吊销或更新这个订户证书，CA 或 RA 可以使用挑战语识别订户的身份。
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

术语	定义
	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。
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。
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。

术语	定义
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)	由网景通信公司开发的、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.
ARL	认证机构 CA 证书的吊销列表

缩写	全称
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	加密套接层协议

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，四川 CA 的 WWW 网站、认证系统的证书服务站点、LDAP、CRL 及 OCSP 服务器构成了四川 CA 认证信息发布的信息库。另外，四川 CA 授权的注册机构的证书服务站点也是认证信息发布的信息库。

2.2 认证信息的发布

2.2.1 CPS 的发布

四川 CA 的认证业务规则可从四川 CA 的网站（www.scca.com.cn）获取；一经网站或以书面声明形式发布、更改，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。

2.2.2 证书和 CRL 发布

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；同时四川 CA 也提供标准的 OCSP 服务，证书的状态信息可通过 OCSP 服务实时获得

2.3 发布的时间或频率

2.3.1 CPS 的发布时间和频率

四川 CA 将及时发布电子认证业务规则（CPS）的最新版本，一旦对规则的修改、补充、调整等获得批准，四川 CA 将在 www.scca.com.cn 上发布，可通过信息库 7X24 小时获得。

四川 CA 根据法律法规、技术进步、业务发展和应用推进的客观要求，决定对 CPS 的改动，其发布时间和频率将由四川 CA 决定。这种发布应该是即时的、高效的，并且是符合国家法律法规的要求。

2.3.2 证书发布时间和频率

对于需要发布的情形，四川 CA 签发的订户证书一经签发即发布到 LDAP 服务器供用户下载，订户可通过证书服务站点获得已签发的证书。通过 OCSP 对证书状态的查询是及时的。

2.3.3 CRL 的发布时间和频率

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。

2.4 信息库访问控制

四川 CA 的安全访问控制机制确保只有经过授权的人员才能编写和修改信息库中的信息，但不限制对这些信息的阅读权。

对于公开发布的 CPS、证书、CRL 等信息，四川 CA 允许公众自行通过网站和目录服务器进行查询和访问。只有经授权的 RA/CA 管理员可以查询电子认证服务机构和注册机构数据库中的其他数据。

3. 身份标识与鉴证

3.1 命名

3.1.1 名称类型

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。

四川 CA 的 CA 证书的签发者和主体域中包含 X. 501 甄别名。四川 CA 的 CA 证书的主体甄别名由表 3 中的内容组成。

表 3- CA 证书主体甄别名属性

属性	值
国家 (C)=	CN
机构 (O)=	四川省数字证书认证管理中心有限公司，或其他机构名称
机构部门 (OU)=	CA 证书中可以包含多个 OU 属性。这些属性可以包含但不限于下列内容： • 部门名称，如：电子商务部 • 证书服务应用类别名，如：电子订单系统 • 其它。
省（市）(S)=	没有使用
地区（L）=	没有使用
通用名 (CN)=	这个属性包括 CA 名。

最终用户证书的主体域中包含一个 X. 501 甄别名，它由表 4 中的内容组成。

表 4 - 最终用户证书主体甄别名属性

属性	值
国家 (C)=	CN
机构 (O)=	组织机构属性使用如下：

属性	值
	- 对于没有确定机构的个人用户证书，是四川省数字证书认证管理中心有限公司。 - 对于其他类型证书，是证书订户所在机构的机构名。
机构部门 (OU)=	CA 证书中可以包含多个 OU 属性。这些属性可以包含但不限于下列内容： - 部门名称，如：电子商务部 - 证书服务应用类别名，如：电子订单系统 - 其它。
省(市) (S)=	订户所在的省，或不用
地区 (L)=	订户所在地区，或不用
通用名 (CN)=	这个属性包括但不限于下列内容： - 域名（服务器证书），或 - 组织机构名（机构证书），或 - 个人姓名（个人证书或机构代表人证书），或 - 假名（电子邮件证书）。
E-Mai 地址 (E)=	e-mail 地址（个人证书，或机构证书）

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。

3.1.2 对名称有意义的要求

个人证书主体甄别名中的通用名通常是个人的真实姓名，或者其他能唯一标识用户身份的其他信息，如个人身份证号码等，它作为标识订户的关键信息被鉴别和认证。

机构证书主体甄别名的通用名通常是组织机构的名称，或者其他能唯一标识该机构的其他信息，如统一社会信用代码等，它作为标识订户的主要信息同其他信息一起被鉴别和认证。

机构代表人证书主体甄别名中的通用名通常是个人的真实姓名，或者其他能唯一标识用户身份的其他信息，如个人身份证号码等，它作为标识订户的主要信息同其他信息（如组织机构名称）一起被鉴别和认证。

场景证书的甄别名通常包含最终签名事件的签名人真实姓名或电子签名场景的特征。

设备证书主体甄别名中的通用名通常是该组织机构的设备名，如域名，它作为标识订户的主要信息同其他信息（如组织机构名称）一起被鉴别和认证。

3.1.3 订户的匿名或伪名

四川 CA 不接受或者允许匿名或者伪名申请，仅接受有明确意义的名称作为唯一标识符。除非在某些具有特殊要求的应用中，可以允许四川 CA 按照一定的规则为用户指定特殊的名称，且四川 CA 能够把该特殊的名称与一个确定的实体（个人、单位）唯一的联系起来。任何这一类特殊的命名，都必须经过四川 CA 安全策略委员会的批准。

3.1.4 理解不同名称形式的规则

依 X. 501 甄别名命名规则解释。

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，可以用其主体名为其签发多张证书，但证书的扩展项不同。

3.1.6 商标的识别、鉴证和角色

证书申请者不应在其证书申请中使用侵害他人知识产权的名称，但四川 CA 并不决定证书申请者是否具有相关知识产权，也无需判断、裁决或解决任何关于域名、名称、商标、服务标的争端问题。当出现此类争端时，四川 CA 有权拒绝或挂起证书申请，直到争端得到有效解决。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

四川 CA 通过使用经数字签名的 PKCS#10 格式的证书请求，验证证书申请者拥有私钥。

场景证书申请人在签名行为发生时，产生证书请求包括申请人的身份信息、证书申请人在进行签名行为时的相关信息（包括证书申请人的签名场景、签名内容或签名内容特征值等）。因此在签名行为发生时证书申请人被视作其私钥的唯一持有者。

3.2.2 机构身份的鉴证

签发机构证书、设备证书时，四川 CA 或其注册机构对组织机构进行身份鉴证，鉴证包括如下两方面内容：

- 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、统一社会信用代码证书等，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。
- 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。

签发服务器证书时，四川 CA 或其注册机构对组织机构进行身份鉴证，鉴证包括如下三方面内容：

- 确认组织机构是确实存在的、合法的实体。确认方式可以是政府签发的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，同时通过权威第三方数据库确认。
- 确认组织机构对域名有所有权或使用权。确认的方式可以是，通过域名注册商确认域名所有者信息。
- 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。

当四川 CA 对外向有关机构（如注册机构或其他授权机构）签发与运营有关的设备证书时，将通过电话或书面形式（包括传真、信函），向该机构的有关责任人确认设备证书申请者来自该机构，且有关申请获得了授权。

3.2.3 个人身份的鉴证

签发个人证书时，四川 CA 或注册机构按照对个人进行身份鉴证，鉴证包括如下两方面内容：

- 确认证书申请者提交的身份信息确实存在且正确，具体方法包括：
 - 采用四川 CA 认可的、提供身份证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、主流的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。
 - 向与其相关的人员（如其员工、客户、合作伙伴）颁发证书的情形，可通过采用包含在该机构业务交易记录或数据库中的信息来完成鉴别。
- 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，如通过订户银行账户进行转帐验证；
 - 验证、确认与该机构相关的证书申请者（如其员工、客户、合作伙伴）的身份及该机构授权其证书申请行为；
 - 其他安全可靠的方式，如面对面等。

若个人证书的身份信息中包含有组织机构信息，则四川 CA 或其注册机构还需要对该组织机构信息进行鉴证，其情形分为如下两种：

若申请者个人直接向四川 CA 或其注册机构提交申请，则四川 CA 或其注册机构，首先按“3.2.2 机构身份的鉴证”所述方法，确认组织机构信息的真实性；然后按“3.2.2 机构身份的鉴证”所述方法，确认申请者属于该组织机构的员工。

若证书申请通过四川 CA 授权的承担注册机构职能的组织机构提交，且证书主体来自该组织机构，则在这种情形下，由组织机构负责确保有关信息的正确性。

3.2.4 场景证书订户身份的鉴证

场景证书订户身份的鉴别参照个人身份鉴别方法，订户在为电子签名行为申请场景证书前，应通过个人身份鉴别，有效证明订户身份，接受场景证书申请的有关条款，同意承担相应的责任。在证书鉴别过程中，由 CA 机构或授权的注册机构，接受订户的证书申

请，对订户的身份真实性进行审核，并采集和记录订户的身份信息和电子签名行为的记录信息。

3.2.5 没有验证的订户信息

四川 CA 不对下列订户信息进行验证：

- 机构部门（OU）
- 电子邮件证书的订户名称
- 证书中指明不验证的其他信息

3.2.6 授权的确认

对于机构证书和设备证书，四川 CA 在签发前，将确认证书申请获得正当授权。确认的方式有多种，如 3.2.2 中对机构授权证书申请者的确认方式。

3.2.7 互操作准则

互操作可能是交叉认证、单身交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各自认证策略的 CA 中心之间建立相互信任关系，从而使双方的订户可以实现互相认证。

四川 CA 将根据业务需要，在遵循本《电子认证业务规则》的各项控制要求的基础上，与四川 CA 证书服务体系中未涉及的其他电子认证服务机构建立交叉认证关系。但交叉认证并不表示四川 CA 批准了或赋予了其他 CA 中心或电子认证服务机构的权力。

3.3 密钥更新请求的标识与鉴证

在订户证书到期前，订户需要获得新的证书以保持证书使用的连续性。四川 CA 一般要求订户产生一个新的密钥对代替过期的密钥对，称作“密钥更新”。然而，在某些情况下，四川 CA 允许订户为一个现存的密钥对申请一个新证书，称作“证书更新”。对于密钥更新而言，订户证书除公钥、有效期和序列号改变外，其他信息都没改变；对于证书更新而言，和密钥更新相比，订户证书公钥也不改变。

3.3.1 常规的密钥更新的标识与鉴证

对于一般正常情况下的密钥更新，订户访问四川 CA 或其注册机构的证书服务站点相应的服务网页进行密钥更新申请，系统自动获取订户原证书的相关信息，如订户甄别名、证书序列号等，形成证书密钥更新申请信息，申请信息包含新公钥并由更新前的私钥签名（对于加密证书密钥更新而言，申请信息不包含新公钥）。

四川 CA 的证书认证系统将对密钥更新申请进行验证，包括验证申请签名，然后进行与新证书申请一样的鉴证。

四川 CA 的场景证书没有密钥更新。

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，也可以来自四川 CA 或其注册机构。证书吊销的方式可以是订户自己吊销，也可以由订户要求四川 CA 或其注册机构管理员吊销，四川 CA 和其注册机构在认为必要的时候，有权发起吊销订户证书。

四川 CA 的场景证书没有证书吊销。

3.4.1 吊销操作

证书用户申请吊销证书时，填写证书吊销申请表，通过一定的方式，如邮寄、邮件、传真等，向四川 CA 或其授权机构提交，并由四川 CA 或其授权机构审核。

3.4.2 吊销申请与确认

证书订户申请吊销证书时候，需通过在线、离线方式向四川 CA 或其授权机构提交申请，四川 CA 或其授权机构根据 3.2.2 或 3.2.3 的鉴证流程对申请者的申请进行鉴别，并进行批准或拒绝的操作。

由四川 CA 或注册机构发起的吊销证书，不需要对订户身份进行标识和鉴别。

如果是司法机关依法提出吊销，四川 CA 将直接以司法机关书面的吊销请求文件作为鉴别依据，不再进行其他方式的鉴别。

3.5 授权服务机构的标识与鉴别

四川 CA 对于授权服务机构，包括注册机构 RA 和证书注册受理点，四川 CA 为其分配账号和操作权限，并对其进行管理。四川 CA 为每一个 RA 签发一张数字证书，作为该 RA 的在证书系统内的唯一身份标识。CA 系统根据 RA 的签名，对 RA 进行身份的鉴别，以判断该 RA 是否为四川 CA 授权注册机构，是否接受其上传的各类服务请求和服务信息。

四川 CA 为每个证书注册受理点的操作员签发一张数字证书，并对其进行管理。CA 系统（包括 RA 系统）根据受理点的签名，对其进行身份的鉴别，以判断该受理点是否为四川 CA 认可的机构，具有何种权限，是否接受其上传的各类服务请求和服务信息。

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。

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。

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。

4.1.2 注册过程与责任

证书申请者可通过四川 CA 的注册服务站点、授权注册机构的注册服务站点现场，或四川 CA 提供的在线申请方式提交各类证书申请，包括相关的身份证明材料。

对于机构证书，注册时申请者须正确填写以下信息：

- 1) 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；
- 2) 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：

- 1) 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；

2) 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:

1) 服务器主机名、域名、IP 地址、或设备名称、及所有者信息等;

2) 申请人信息, 如姓名、电话、邮件地址等。

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 测试证书的申请处理

测试证书由四川 CA 或授权注册机构为用户制作, 仅供用户非正式用途的测试使用。四川 CA 对用户的申请信息不做鉴别验证, 不承担任何证书真实性的责任, 也不承担因为申请者填写的信息泄漏引起的任何责任。

四川 CA 对测试证书有严格的规定, 证书主题中用户名需加以英文 “test” 或者中文 “测试” 标识, 而且证书有效期限不超过 12 个月。

4.2.2 执行识别与鉴别功能

四川 CA 或其注册机构按照本《电子认证业务规则》所规定的身份鉴别流程对申请人的身份进行识别与鉴别。

对于机构证书和设备证书, 四川 CA 及其注册机构按本 CPS3.2.2 所述的方式对组织机构及其授权申请人进行识别和鉴别。

对于个人证书的申请, 四川 CA 及其注册机构按本 CPS3.2.3 所述的方式对订户进行识别和鉴别。

4.2.3 证书申请批准和拒绝

四川 CA 或其注册机构根据本《电子认证业务规则》所规定的身份鉴别流程对证书申请人身份进行识别与鉴别后, 根据鉴别结果决定批准或拒绝证书申请。

如果证书申请人通过本《电子认证业务规则》所规定的身份鉴别流程且鉴证结果为合格，四川 CA 或其注册机构将批准证书申请，为证书申请人制作并颁发数字证书。

证书申请人未能通过身份鉴证，四川 CA 或注册机构将拒绝申请人的证书申请，并通知申请人鉴证失败，同时向申请人提供失败的原因（法律禁止的除外）。

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

4.2.4 处理证书申请的时间

四川 CA 及注册机构将在合理时间内完成证书请求处理。在申请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 5 个工作日。

对于场景证书等扩展业务的申请，即时处理。

4.3 证书签发

4.3.1 证书签发中 RA 和 CA 的行为

作为证书认证系统的运营者，四川 CA 既是一个 CA，同时也承担了部分 RA 的职能（如负责设备证书的注册、审批等）。另外，四川 CA 授权的机构也承担相应的 RA 职能，如接收、处理证书服务请求。

在证书签发前 RA 管理员负责证书申请的鉴证，在证书申请通过鉴证后，RA 管理员将批准证书请求。在批准证书申请时，RA 管理员使用证书登录到 RA 系统，查询系统记录的有关请求并批准该请求。批准的信息将会发送到四川 CA 的 CA 系统，CA 系统签发证书并返回给 RA 系统供证书申请者下载。

4.3.2 CA 和 RA 对订户的通知

电子认证服务机构通过注册机构，对订户的通告有以下几种方式：

- 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；
- 通过已经确认安全的通道通知；
- 其他四川 CA 认为安全可行的方式通知订户。

4.4 证书接受

4.4.1 构成接受证书的行为

订户完成申请流程后，四川 CA 或其注册机构经审核通过将载有证书和私钥的介质、或者证书获得方式、或者与证书相关的密码交付给订户，即意味着订户已经接受了证书。订户接受数字证书后，应妥善保管证书和私钥。

以下行为被认为订户已经接受了证书：

- 订户通过面对面的方式从四川 CA 或其注册机构接受载有证书和私钥的介质；
- 订户通过网络获取证书的指示信息，将证书下载或安装到本地存放介质，如 IC 卡、USBKey 或其他符合规范的存储介质，系统记录订户下载了证书即表明订户接受了证书；
- 订户使用场景证书完成特定场景中的电子签名时即被视为同意接受证书；
- 订户接受了获得证书的方式，5 个工作日内没有提出反对证书或者证书中的内容。

4.4.2 CA 对证书的发布

四川 CA 有基于 LDAP 协议的目录服务，除以下情形外，四川 CA 默认将证书信息发布到 LDAP 目录服务系统：

- 对于一次性使用的数字证书，四川 CA 不发布证书信息；
- 对于用户明确表示拒绝发布证书信息的，四川 CA 不发布证书信息。

4.4.3 CA 对其他实体的通告

对于其签发的证书，四川 CA 及其注册机构不通知其他实体。其他实体可以通过从目录服务器中查询四川 CA 已经签发的数字证书。

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 业务规则保障的。

4.5.1 订户私钥和证书使用

对于签名证书，其私钥可用于对信息的签名。在可能的情况下，签名证书及信任链上的证书（根证书除外）应同被签名信息一起提交给依赖方。证书持有者使用私钥对信息签名时，应该被告知并确认签名的内容。对于具有身份鉴别用途的证书，其私钥可用于对鉴别方提交的挑战信息进行签名；在可能的情况下，具有身份鉴别用途的证书及信任链上的证书（根证书除外）应提交给验证方。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。证书持有者应妥善保管其证书私钥。

4.5.2 依赖方公钥和证书使用

当依赖方接受到经数字签名的信息后，应该，

- (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) 检验证书的有效性，确认该证书在有效期之内，且该证书没有被吊销；
- (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。

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，须先通过适当的途径获得接收方的加密证书，然后使用证书上的公钥对信息加密。依赖方应将加密证书连同加密信息一起发送给接收方。

4.6 证书更新

4.6.1 证书更新的情形

对于四川 CA 签发的任何最终用户证书，证书到期前 60 天系统将会自动发邮件给订户提醒用户证书将到期，如需继续使用可进行证书更新。到期前 60 天内，如果订户原来的注册信息继续有效，订户可访问四川 CA 或注册机构的证书更新站点申请证书更新。申请证书更新时用户无需象初次申请那样填写注册信息，系统会自动获取所需的信息。证书更新可以更换密钥对，也可以使用原有密钥对，视更新的具体情形而定，关于证书更新与重新申请一个同样主体甄别名的新证书区别见 3.3。

若用户需要改变注册信息，则不能更新证书，需按新证书申请流程进行。

证书到期或吊销后，将无法进行更新，只能按照初始流程重新申请证书。

4.6.2 请求证书更新的实体

订户可以请求证书更新。订户包括持有四川 CA 签发的个人、机构及设备等各类证书的证书持有人。

4.6.3 证书更新请求的处理

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：

- 确认、验证申请对应的原证书存在并且由四川 CA 认证机构签发；
- 证书更新请求在允许的期限内；
- 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。

对于机构证书和设备证书根据用户以前提交的注册信息，按与新证书申请一样的流程完成证书申请的鉴证，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。在进行鉴证时，若机构用户以前提交的机构身份证明文件仍在有效期内，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。完成以上鉴证后，批准更新请求，签发新证书。

以上过程可以是离线或在线的。

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（如支付了有关费用），则证书更新请求将获得批准，新证书将获得签发。以上过程可以是自动或手动的。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：

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

以上过程可以是自动或手动的。

对于更换密钥的证书更新，参见 4.7.3。

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

证书密钥更新即产生新的密钥对，使用与原证书一样的主体甄别名并由同一签发者签发新证书。

4.7.1 证书密钥更新的情形

对于四川 CA 签发的任何最终用户证书，证书到期前 60 天系统将会自动发邮件给订户提醒用户证书将到期。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，则订户可以申请证书密钥更新。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，因此，证书密钥更新是改变证书密钥对的证书更新。在证书到期前 60 天起，订户可向四川 CA 或注册机构申请证书密钥更新。申请证书密钥更新时用户无需象初次申请那样填写注册信息，系统会自动获取所需的信息。

证书密钥更新的具体情形如下：

- 当订户证书即将到期或已经到期时；
- 当订户证书密钥遭到损坏时；
- 当订户证实或怀疑其证书密钥不安全时；
- 其它可能导致密钥更新的情形。

场景证书仅用于订户特定一次的电子签名行为，没有证书更新和证书密钥更新。

证书吊销后不允许证书密钥更新。

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

对于证书密钥更新请求，用户提交的证书签名请求（PKCS#10）包含有新的公钥，并由新私钥签名；同时，证书签名请求中还包含有用原证书私钥签名的更新请求信息。

接收到用户的证书密钥更新请求后，四川 CA 认证系统会自动完成如下验证操作：

- 确认、验证申请对应的原证书存在并且由四川 CA 认证机构签发；
- 证书更新请求在允许的期限内；
- 用订户新的公钥对证书签名请求进行签名验证；
- 用原证书的公钥对证书签名请求中的、使用原证书私钥签名的有关更新请求信息进行签名验证。

以上自动验证通过后，四川 CA 或其注册机构按与证书更新相同的方式和流程（参见 4.6.3）完成证书密钥更新请求的鉴证、批准，签发新的证书。

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

证书变更是指在证书未到期之前，更改除公钥及有效期之外的其他信息。四川 CA 允许订户进行证书变更，对原证书进行吊销处理。如果需要变更证书中的主题信息，订户需要提交相关鉴证材料，鉴证流程同 3.2。

场景证书没有证书变更。

4.8.2 请求证书变更的实体

原证书订户。

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

(1) 发生下列情形之一的，订户应当申请吊销数字证书：

- 数字证书私钥泄露；
- 数字证书中的信息发生重大变更；
- 认为本人不能实际履行数字证书认证业务规则。

(2) 发生下列情形之一的，四川 CA 可以吊销其签发的数字证书：

- 四川 CA 或其注册机构有理由相信订户违背了订户协议下的义务、陈述或担保；
- 四川 CA 或其注册机构有理由相信数字证书的安全性得不到保证；
- 四川 CA 或其注册机构和订户达成的订户协议已经终止；
- 四川 CA 或其注册机构有理由相信证书申请中的信息有违背事实的错误；
- 除了未经鉴证的订户信息外，包含在证书中的信息不正确或已经改变；
- 订户请求吊销证书；
- 法律、行政法规规定或法院申请的其他情形。

4.9.2 请求证书吊销的实体

以下实体可以请求吊销订户证书：

- 四川 CA、注册机构或证书订户可以在 4.9.1 所述情形下要求吊销订户证书。
- 对于个人证书，证书订户可以随时根据自己的意愿请求吊销自己的证书。
- 对于机构证书，组织机构授权的代表有资格请求吊销签发给组织机构的证书。
- 对于设备证书，拥有该设备证书的组织机构授权的代表有资格请求吊销已经签发的证书。
- 政府主管机构、其他有关部门或者法院依照正式合法的程序提出申请。

4.9.3 吊销请求的流程

当四川 CA 或其注册机构有充分的理由相信需要吊销订户的证书时，四川 CA 或其注册机构的有关人员可以通过内部确定的流程提请吊销证书。在证书吊销后，四川 CA 或其注册机构将通过适当的方式，包括邮件、传真等，通知订户证书已被吊销及被吊销的理由。

订户可以通过以下方式要求吊销自己的证书：

- 前往四川 CA 或注册机构现场书面提出申请，出具相关机构授权及个人的身份证明材料；
- 访问四川 CA 或注册机构提供的证书服务网页，通过在线提交吊销请求；
- 通过电子邮件、传真、特快专递等可靠的方式告知四川 CA 或其注册机构。

四川 CA 或授权的注册机构根据 3.2 的要求对订户提交的吊销请求进行审核，审核通过并吊销订户证书后，注册机构将以适当的方式如当面通知、邮件、传真等方式通知订户证书被吊销。

场景证书没有证书吊销。

4.9.4 吊销请求宽限期

当订户发现出现 4.9.1 中的情况时，应该尽快提出吊销请求，从发现需要吊销证书到向四川 CA 或其注册机构提出吊销请求的时间间隔的要求如下，

- 对于个人证书不能超过 8 小时。
- 对于机构证书和设备证书不能超过 4 小时。

4.9.5 CA 处理吊销请求的时限

四川 CA 或注册机构从接到吊销请求到完成处理请求的时间如下：

- 对于个人证书不能超过 8 小时。
- 对于机构证书和设备证书不能超过 8 小时。

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。如果进行证书的状态检查，必须使用以下两种之一进行证书的状态查询：

- CRL 查询：利用证书中标识的 CRL 地址，进行证书状态的检验。
- 在线证书状态查询（OCSP）：服务系统接受证书状态查询请求，从目录服务器中查询证书的状态，经签名后返回查询结果。

依赖方要验证 CRL 的可靠性和完整性，确保是四川 CA 发布并签名的。

4.9.7 CRL 发布频率

四川 CA 的认证系统每天零时为证书签发 CA 产生证书吊销列表。对于特别的证书签发 CA，四川 CA 可定制证书吊销列表产生的频率。

四川 CA 认证服务机构 CA 证书的 CRL（即 ARL）至少每年发布一次，当有 CA 证书被吊销时，吊销当日及时发布。

4.9.8 CRL 发布的最大滞后时间

一个证书从它被吊销到它被发布到 CRL 上的滞后时间不超过 24 小时。

4.9.9 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。

4.9.10 在线状态查询要求

依赖方应检查证书的吊销状态。如果依赖方未通过 CRL 方式查询，则应通过 OCSP 在线方式查询。

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

无论订户还是四川 CA、注册机构，发现证书密钥受到安全损害时应立即吊销证书。

4.9.13 证书挂起的情形

目前，四川 CA 不提供证书挂起服务。一旦提供挂起服务，四川 CA 将会通过网站等进行公布。

4.10 证书状态服务

四川 CA 通过网站 CRL、OCSP、LDAP 提供证书状态服务。

对于被吊销证书，其状态将同时在 CRL、OCSP 反映。

4.10.1 操作特征

四川 CA 提供的证书状态查询以网络服务的形式：

- CRL 通过 80 端口采用 HTTP 协议提供；
- OCSP 符合 RFC2560，反映证书的当前状态；
- 证书目录 LDAP 符合 LDAPV3（RFC3377，2251-2256，2829-2830）。

4.10.2 服务可用性

四川 CA 的 CRL、OCSP 证书状态服务均保证 7X24 小时可用，并且采用了冗余技术。

4.10.3 可选特征

无。

4.11 订购结束

（1）订购结束是指证书到期或证书吊销后，该证书的服务时间结束。

订购结束包括以下情形：

- 证书有效期满，订户不再延长证书使用期或不再重新申请证书时，订户终止订购。
- 在证书有效期内，证书被吊销后，即订购结束。
- 政府主管机构、其他有关部门或者法院依照正式合法程序提出申请。

（2）订购结束流程

- 订户不再延长证书使用期或不再重新申请证书的，有效期满后订购自动结束。四川 CA 定期对订购结束后的证书及相应订户数据进行 5 年以上的归档保留管理。
- 四川 CA 或其注册机构、证书订户、政府主管机构、其他有关部门或法院在证书有效期内申请终止使用四川 CA 的证书认证服务，四川 CA 或其注册机构批准终止请求后，将该订户的证书在 8 小时内吊销，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 5 年以上的归档保留管理。

4.12 密钥托管与恢复

四川 CA 依国家密码管理部门的相关规定，提供加密证书密钥的集中产生、保存和恢复。

4.12.1 密钥托管与恢复的策略与行为

订户加密证书密钥对可以由四川 CA 的密钥管理系统集中安全产生和保存，密钥恢复是一种严格受控的过程，只有在如下情况下才允许进行密钥恢复：

- 证书持有者提出申请；
- 国家执法、司法机构因执法、司法的需要；
- 国家其他管理部门管理需要。

密钥恢复只有在必须的情况下才进行，并且申请要提出充分的理由和提供有关文件、材料。

4.12.2 会话密钥的封装与恢复的策略与行为

会话密钥是指用户在使用证书建立加密通道时临时生成的加密密钥，该密钥由应用环境来决定使用，四川 CA 不对其进行保存和恢复。

5. 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

四川 CA 的 CA 机房位于成都市电子政务统一数据中心内，地址是高新区锦城大道 366 号民丰楼 4 号楼 5 层。

四川 CA 认证业务的运营场地是按照国家相关规范进行构建的，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，可以阻止未经授权的进入、穿透。敏感区域只设置一个门作为的常规入口。根据消防要求置了消防紧急出口。敏感区域及以上区域没有窗口。

运营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，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，。

四川 CA 认证机构的运营场地能达到以下安全和控制风险要求：

- 防止未经授权的物理访问

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 认证机构内的受限制区域。

- 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。

5.1.2 物理访问控制

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。

5.1.3 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 认证机构还具有新风/空调系统控制运营设施中的温度和湿度。

5.1.4 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。

5.1.5 火灾防护

5.1.5.1 结构防火

四川CA认证机构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。

5.1.5.2 火灾报警及消防设施

- 四川 CA 认证机构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。

5.1.5.3 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。

5.1.6 介质存储

四川 CA 认证机构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。

5.1.8 异地备份

四川 CA 认证机构对关键系统数据、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。

5.1.9 注册机构物理控制

四川 CA 注册机构的物理场地有足够的安全措施，保证只有授权的人员才能进入，只有授权的人员才能接触系统进行证书管理。

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 对影响证书生命周期管理操作的有关人员定为可信角色，四川 CA 可信人员包括：

- 安全策略委员会成员
- CA 系统管理人员
- 系统维护管理人员
- 运维管理人员
- 网络安全管理人员
- 物理环境安全管理人员
- 数据库管理人员
- 密钥管理员
- 秘密分管者
- 可信雇员管理人员
- 运营审计人员
- 鉴别验证人员
- 用户档案管理人员

5.2.2 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。
- CA 秘密共享持有者采用 m of n 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。

5.2.3 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。

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：

- CA 系统管理人员
- 系统维护管理人员
- 运维管理人员
- 网络安全管理人员
- 物理环境安全管理人员
- 数据库管理人员
- 密钥管理员
- 秘密分管者
- 鉴别验证人员

5.3 人员控制

5.3.1 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、培训及工作经历应足够胜任其工作，所有入职即签订保密协议。

四川 CA 客服人员必须受过专门的服务技能培训，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如下要求：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。

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。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 将拒绝应聘人员获得有关职位或取消已雇用人员的可信资格。

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。
 - 密码设备生命周期的管理事件，例如接收、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。
 - 成功或失败的证书操作。

这些记录由认证系统自动记录，保存在数据库。

- 系统安全事件，包括，
 - 成功或不成功访问 CA 系统的活动。
 - 对于 CA 系统网络的非授权访问及访问企图。
 - 系统崩溃，硬件故障和其他异常。
 - 防火墙和路由器记录的安全事件。
 - 系统启动和关闭。

这些记录由操作系统自动完成，四川 CA 的系统维护人员会定期检查系统日志。

- 四川 CA 物理设施的访问记录，如，
 - 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。

- 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

日志记录包括如下信息：

- 每个日志记录的日期和时间。
- 对于自动日志记录，登记的序列号或序号。

- 做日志记录的实体的身份。
- 日志记录的种类。

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 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。

5.4.5 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。

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

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。

5.4.8 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，要及时进行相应的处理和解决。

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、磁带、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，有操作人员手工记录；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

四川 CA 中的档案收集系统由人工操作或自动操作两部分组成。

5.5.7 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。

5.6 CA 密钥变更

当 CA 密钥对的累计寿命超过 6.3.2 中规定的最大生命期，四川 CA 将启动密钥更新流程，替换已经过期的 CA 密钥对。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。

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。

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 CA 证书或其受委托的 CA 证书出现私钥损害时，四川 CA 将立即吊销该 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。

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

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。

6.1.1.2 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 USBKey）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 USBKey）产生。

6.1.2 私钥传送给订户

四川 CA 各类 CA 证书密钥对由四川 CA 数字认证中心在其运营场地产生，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 USBKey）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最终用户在约定的密码硬件中

（如 USBKey）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。

6.1.3 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格式，以电子的方式将公钥提交给四川 CA（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。

6.1.4 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。

6.1.5 密钥的长度

四川 CA 的 CA 和订户密钥对至少是 256 位 SM2。

6.1.6 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。

6.1.7 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。证书中的密钥用法扩展项按表 5 所示设定：

表 5 - 密钥用法扩展项的设置

		CA 证书	机构证书	个人证书	服务器证书	运营设备证书
Criticality		非关键	非关键	非关键	非关键	非关键
0	digitalSignature	未设置	设置	设置	设置	设置
1	nonRepudiation	未设置	设置	设置	未设置	未设置
2	keyEncipherment	未设置	设置	设置	设置	设置
3	dataEncipherment	未设置	设置	设置	设置	未设置
4	keyAgreement	未设置	设置	设置	设置	未设置
5	KeyCertSign	设置	未设置	未设置	未设置	未设置
6	CRLSign	设置	未设置	未设置	未设置	未设置
7	EncipherOnly	未设置	未设置	未设置	未设置	未设置
8	DecipherOnly	未设置	未设置	未设置	未设置	未设置

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 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，并妥善保管、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

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。

6.2.3 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。

6.2.4 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和异地灾难恢复备份。

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。

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 6.2.10 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；但对某些特别的运营设备证书，如时间戳证书，四川 CA 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。

6.2.6 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。

6.2.7 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、国家密码主管部门认可的密码模块中（如 USBKey），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。

6.2.8 激活私钥的方法

6.2.8.1 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。

6.2.8.2 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，需要专门的的安全管理人员输入保护口令后才能激活。

6.2.8.3 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 6.2.2 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。

6.2.9 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 及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。

6.2.10 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，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授权使用。若私钥吊销、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。

6.2.11 密码模块的评估

由国家密码管理部门负责。

6.3 密钥对管理的其他方面

6.3.1 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。

6.3.2 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。

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：

- 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；
- 不能和操作员的姓名相同；
- 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

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。

6.4.3 激活数据的其他方面

6.4.3.1 激活数据的传送

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，不应传递给其他人员，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 或其注册机构，有可能代订户在特定的密码硬件（如 USBKey）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。

6.4.3.2 激活数据的销毁

存有四川 CA 的 CA 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 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。

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权威机构的安全测评、评审，并获得了相应资质。

6.6 生命周期技术控制

6.6.1 系统开发控制

四川 CA 通过内部流程来控制证书认证系统的研发工作，并确保该系统安装的可靠性。

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 CA 运营系统进行安全管理。

6.6.3 生命期的安全控制

四川 CA 的证书认证系统在系统设计过程中充分进行了安全性考虑，在开发过程中有严格的流程进行代码安全管理，在开发完成后进行了严格的安全测试，在正式使用前通过了国家有关部门的系统安全性审查。

6.7 网络的安全控制

四川 CA 证书认证系统网络进行安全漏洞扫描和安全优化，部署了防火墙、入侵检测系统，并在系统通信过程中使用加密和数字签名进行保护。

6.8 时间戳

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. 证书、CRL 和 OCSP

7.1 证书

四川 CA 签发的证书符合(a)ITU-TX.509v3 4-edition (2001)：信息技术-开放系统互连-目录：认证框架（1997 年 6 月）标准；(b) RFC 3280：Internet X.509 公钥基础设施证书和 CRL 结构（1999 年 1 月）。

证书至少包含基本的 X.509v1 域，其规定值或值的限制如表 6 所描述。

表 6 - 证书结构的基本域

域	值或值的限制
版本	V3
序列号	每个证书唯一的值
签名算法	用于签证书的算法的名称（见 CPS7.1.3）
签发者 DN	签发者的甄别名。
有效期从	基于国际通用时间(UTC)，和北京时间同步，按 RFC3280 要求编码
有效期至	基于国际通用时间(UTC)，和北京时间同步，按 RFC3280 要求编码。有效期限的设置符合 CPS6.3.2 规定的限制
主体 DN	证书持有者或实体的甄别名。
公钥	根据 RFC3280 编码，使用 CPS7.1.3 中指定的算法，密钥长度满足 CPS6.1.5 指定的要求。
签名	生成和编码满足 RFC3280 的要求。

7.1.1 版本号

X.509v3 证书。

7.1.2 证书扩展项

针对特别的用户，四川 CA 签发的证书有可能包含私有扩展项，不能识别私有扩展项的应用、依赖方可以忽略该扩展项。

7.1.2.1 密钥用法 (Key Usage)

该扩展项指定证书密钥对的用法，不同证书该扩展项的设置见 6.1.7。

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。这个扩展项的 criticality 域设置为 FALSE。

7.1.2.3 主体备用名 (subjectAltName)

未使用。

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。最终用户证书的基本限制扩展项的主体类型设为最终实体 (End-Entity)。

CA 证书的基本限制扩展项中的路径长度设定为在证书路径中该证书之后的 CA 级数。对于最终用户证书签发 CA，其 CA 证书 “pathLenConstraint” 域的值设为 0，表示证书路径中仅有一个最终用户证书可以跟在这个 CA 证书后面。

7.1.2.5 扩展的密钥用法 (Extended Key Usage)

对四川 CA 不同的证书，扩展的密钥用法扩展项设定如下。

表 7 - 可扩展的密钥用法扩展项的设置

		服务器证书	个人/机构证书
Criticality		非关键	非关键
0	ServerAuth	设置	未设置
1	ClientAuth	设置	设置

		服务器证书	个人/机构证书
2	CodeSigning	未设置	未设置
3	EmailProtection	未设置	未设置
4	IpssecEndSystem	未设置	未设置
5	IpssecTunnel	未设置	未设置
6	IpssecUser	未设置	未设置
7	TimeStamping	未设置	未设置
8	OCSP Signing	未设置	未设置
-	Microsoft Server Gated Crypto (SGC) OID: 1.3.6.1.4.1.311.10.3.3	设置	未设置
-	Netscape SGC - OID: 2.16.840.1.113730.4.1	设置	未设置
-	TBD - OID: 2.16.840.1.113733.1.8.1	未设置	未设置

7.1.2.6 CRL 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。此扩展项的 criticality 项应设为 FALSE。

7.1.2.7 签发 CA 密钥标识符

四川 CA 最终用户证书及中级 CA 证书中有签发 CA 密钥标识符扩展项，当证书签发者包含主体密钥标识扩展项时，签发 CA 密钥标识符由签发证书的 CA 的公钥进行哈希运算后的值构成；否则，它将包含签发 CA 的主体 DN 和序列号。这个扩展项的 criticality 域设置为 FALSE。

7.1.2.8 主体密钥标识符

当证书包含主体密钥标识符扩展项时，该值由证书主体的公钥产生。使用该扩展项时，其扩展项的 criticality 域设为 FALSE。

7.1.3 密钥算法对象标识符

四川 CA 签发的证书按照 RFC 3280 标准，使用 SM2 Signing with SM3 (1.2.156.10197.1.501) 算法签名。

7.1.4 名称形式

四川 CA 签发证书的甄别名符合 X500 关于甄别名的规定。对于证书主体甄别名，0 代表证书持有者所在的组织机构，第一个 OU 代表证书持有者所在的部门。

对于证书签发者甄别名，0 代表证书签发机构，第一个 OU 签发机构中的部门或服务类。甄别名可以包含不止一个的 OU 用于存放其他信息。

7.1.5 名称限制

除非某些特殊要求的应用场景，四川 CA 签发的证书中的通用名不能使用假名、伪名。

7.1.6 证书策略对象标识符

未使用。

7.1.7 策略限制扩展项的用法

没使用。

7.1.8 策略限定符的语法和语义

没有规定。

7.1.9 关键证书策略扩展项的处理规则

与 ITU X.509 和 RFC3280 规定一致。

7.2 CRL

四川 CA 认证系统签发的 CRL 符合 RFC3280 标准。CRL 至少包含如表 8 所述基本域和内容。

表 8 - CRL 结构的基本域

域	值或值的限制
版本	V2
签名算法	签发 CRL 的算法。使用 SM2 Signing with SM3 (1.2.156.10197.1.501) 算法签名。
颁发者	签发 CRL 的实体。颁发者甄别名。

域	值或值的限制
有效期	CRL 的签发日期。
下次更新	CRL 下次签发的日期。
吊销的证书	列出吊销的证书，包括吊销证书的序列号和吊销日期。

7.2.1 版本号

V2。

7.2.2 CRL 和 CRL 条目扩展项

与 ITU X. 509 和 RFC3280 规定一致。

7.3 OCSP

四川 CA 认证系统签发的 OCSP 响应符合 RFC2560 标准。OCSP 响应至少包含如表 9 所述基本域和内容。

表 9 - OCSP 结构的基本域

域	值或值的限制
状态	响应状态，包括成功、请求格式错误、内部错误、稍候重试、请求没有签名和请求签名证书无授权，当状态为成功时必须包括以下各项。
版本	V1
签名算法	签发 OCSP 的算法。
颁发者	签发 OCSP 的实体。
产生时间	OCSP 响应的产生时间。
证书状态列表	包括请求中所查询的证书状态列表。每个证书状态包括证书标识、证书状态以及证书吊销信息。
证书标识	包括数据摘要算法、证书甄别名数据摘要值、证书公钥数据摘要值和证书序列号。
证书状态	证书的最新状态，包括有效、吊销和未知。
证书吊销信息	当返回证书状态为吊销时包含吊销时间和吊销原因。

7.3.1 版本号

V1。

7.3.2 OCSP 扩展项

与 RFC2560 一致。

8. 认证机构审计和其他评估

四川 CA 在物理控制、密钥管理、操作控制、证书生命周期管理等方面的执行等情况将被审查、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，并根据审查结果采取行动。

8.1 评估的频率和情形

审计是为了检查和监督四川 CA 及其注册机构或其它关联机构，是否依据《中华人民共和国电子签名法》、《电子认证服务管理办法》、《四川 CA 电子认证业务规则》的要求，依法开展电子认证服务业务，以及在开展业务过程中，是否存在违反其它法律法规与四川 CA 的业务规范、管理制度、安全策略等情况，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：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或四川 CA 委托的第三方机构对自身的电子认证服务业务进行审计与评估。审计内容、评估标准及审计评估结果是否公开由主管部门确定。

内部审计是指四川 CA 自行组织人员对机构内部、下属机构等进行审计评估，审计结果供四川 CA 内部用以完善管理、改进服务，不需对外公开。内部审计按四川 CA 自身需求确定频率。

8.2 评估者的资质

对四川 CA 实施规范审计的审计者所具有的资质和经验必须符合监管法律和行业准则规定的要求，包括：必须是经许可的、有营业执照的、具有计算机安全专门技术知识的审计人员或审计评估机构，且在业界享有良好的声誉。了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和操作。具备检查系统运行性能的专业技术和工具。

内部审计人员的选择一般包括：四川 CA 的安全负责人及安全管理人员、四川 CA 业务负责人、认证系统及信息系统负责人、人事负责人、其他需要的人员。

四川 CA 无条件接受主管部门的评估。对四川 CA 实施评估的评估者所具有的资质由主管部门决定。

8.3 评估者与被评估者之间的关系

评估者为电子认证服务的主管部门选择的独立第三方人员，与四川 CA 不存在任何商业利益关系。

四川 CA 委托的第三方机构评估者应是四川 CA 无任何业务、财务往来或其他足以影响评估客观性的利害关系的机构或组织。

8.4 评估的内容

评估内容包括：CA 物理环境和控制、CA 基础控制、密钥管理操作、证书生命周期管理、CA 业务规则、CPS 执行情况。

8.5 对问题与不足采取的措施

四川 CA 管理层将对审计报告进行评估，对在一致性审计中发现的重大意外或不作为积极采取补救措施，直到问题解决。从完成审计到采取行动纠正问题不超过 30 天。

8.6 评估结果的传达与发布

电子认证服务主管部门的年度审查结果将在其相关网站上公开，任何人均可查询。

其他评估结果除非法律或主管部门明确要求，四川 CA 一般不公开评估结果。

8.7 其他评估

除了电子认证服务主管部门的年度审计外，四川 CA 将定期进行内部审计评估，审计评估的内容与外部审计一致。

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 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。

9.1.2 证书查询的费用

四川 CA 目前不对证书查询收取专门的费用。

9.1.3 证书吊销或状态信息的查询费用

证书吊销和吊销列表（CRL）的获取不收取费用。四川 CA 有可能根据需要将 OCSP 服务作为增值服务收取费用。

9.1.4 其他服务费用

四川 CA 根据市场与证书实际应用的需要确定。

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。

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 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 9.9）。

9.2.2 其他资产

四川 CA 具备国家信息产业主管部门所规定的资金实力，具备承担赔偿责任的条件。

9.2.3 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最终实体主要是证书订户和证书依赖方。

9.3 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。

9.3.1 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；
- 用户与认证机构、注册机构签订的协议；

9.3.2 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。

9.3.3 保护保密信息的责任

四川 CA 不但有各种严格的管理制定、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方面的培训。

9.4 个人隐私保密

9.4.1 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。

9.4.2 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。

9.4.3 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。

9.4.4 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。

9.4.5 使用隐私信息的告知与同意

四川 CA 或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。

9.4.6 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 及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。

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。

9.5 知识产权

9.5.1 证书和吊销信息中的知识产权

四川 CA 对它签发的证书、证书吊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。

9.5.2 CPS 中的知识产权

四川 CA 对本 CPS 拥有知识产权。

9.5.3 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。

9.5.4 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。

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的承诺如下：

- 遵守《中华人民共和国电子签名法》及相关法律的规定，接受主管部门的领导，对签发的数字证书承担相应的法律责任；
- 四川 CA 保证使用的系统及密码符合国家政策与标准，保证其 CA 本身的签名私钥在内

部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定；

- 除非已通过四川 CA 发出了 CA 的私钥被破坏或被盗的通知，四川 CA 保证其私钥是安全的；
- 四川 CA 签发给订户的证书符合四川 CA 的 CPS 的所有实质性要求；
- 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的证书的有效性和可靠性事件；
- 证书公开发布后，CA 机构向证书依赖方证明，除未经验证的订户信息外，证书中的其他订户信息都是准确的。

9.6.2 RA 的陈述与担保

四川 CA 授权的注册机构在参与电子认证服务过程中的承诺如下：

- 提供给证书订户的注册过程完全符合四川 CA 的 CPS 的所有实质性要求；
- 在生成证书时，不会因为注册机构的失误而导致证书中的信息与证书申请人的信息不一致；
- 注册机构将按本 CPS 规定，及时向四川 CA 提交证书申请、吊销、更新等服务请求。

9.6.3 订户的陈述与担保

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

- 订户已熟悉本《电子认证业务规则》的条款和与其证书相关的证书政策，还需遵守证书使用方面的有关限制；
- 订户提供的，申请表所填的信息，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。
- 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吊销；
- 订户对自己的私钥保管采取了安全、合理的措施实现有效保护，防止证书私钥遗失、泄露和被篡改；

- 一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄密以及其他情况，订户应立刻通知四川 CA 或注册机构，申请采取吊销等处理措施。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉本《电子认证业务规则》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《电子认证业务规则》的有关条款。依赖方对未履行《电子认证业务规则》中规定的依赖方义务而带来的后果承担法律责任。

9.6.5 其他参与者的陈述与担保

其他参与者的陈述与担保同9.6.4。

9.7 担保免责

四川 CA 不对其签发的证书适用于其规定目的以外的任何应用承担任何担保，对证书在其规定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。

9.8 有限责任

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、吊销（错误）证书、经济赔偿。

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

9.9 赔偿

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的，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吊销。

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。

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 CPS 提前终止，在四川 CA 颁布新版本 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。

9.10.3 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。

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 CACPS 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 将修改了的 CPS 通过四川 CA 网站关于四川 CA 中的业务声明 CPS 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，合理的时间应保证有关方面受到的影响最小。

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 有重要缺陷时，必须修改《电子认证业务规则》。

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协商解决，协商解决不了的，可通过法律解决。四川 CA 订户协议、依赖方协议和其他订户协议已包括该项内容。

9.14 管辖法律

中华人民共和国法律、规则、规章、法令和政令将管辖四川 CA 的业务活动。四川 CA 的任何业务活动受有关法律、法规的制约，任何业务和法律文件、合同的解释、执行不能同有关法律、法规相冲突。

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、合同法、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，胜讼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

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。

9.17 其他条款

四川 CA 对本《电子认证业务规则》拥有最终解释权。