

ZJCA 电子认证业务规则

V 3.0

浙江省数字安全证书管理有限公司

2009 年 5 月

版权声明

浙江省数字安全证书管理有限公司拥有本规则的完全版权。

其他任何个人和团体可准确完整地转载、粘贴或发布本规则。

任何个人和团体不得部分的转载、粘贴或发布本规则，更不得更改本规则的部分词汇进行转贴。

本规则的最新版本请参见本公司网页 <http://www.zjca.com.cn>，或者联系浙江省数字安全证书管理有限公司。

地址：浙江省杭州市中山北路 631 号晶晖商务大厦 22 层

邮编：310014

电话：86-571-85800770（总机）

传真：86-571-85800770-116

电子邮件：zjca@zjca.com.cn

本规则如有改动，对特定对象不再另行通知。

目 录

版权声明	1
1.概括性描述	12
1.1 概述	12
1.2 文档名称与标识	13
1.3 电子认证活动参与者	13
1.3.1 电子认证服务机构	13
1.3.2 注册机构	13
1.3.3 订户	14
1.3.4 依赖方	14
1.3.5 其他参与者	14
1.4 证书应用	14
1.4.1 适合的证书应用	14
1.4.2 限制的证书应用	16
1.5 策略管理	17
1.5.1 策略文档管理机构	17
1.5.2 联系人	17
1.5.3 决定 CPS 符合策略的机构	17
1.5.4 CPS 批准程序	17
1.6 定义和缩写	18
2.信息发布与信息管理	18
2.1 认证信息的发布	18
2.2 发布的时间或频率	19
2.3 信息库访问控制	19
3. 身份标识与鉴别	19
3.1 命名	19
3.1.1 名称类型	19
3.1.2 对名称意义化的要求	19

3.1.3 订户的匿名或伪名	20
3.1.4 理解不同名称形式的规则	20
3.1.5 名称的唯一性	20
3.1.6 商标的识别、鉴别和角色	20
3.2 初始身份确认	20
3.2.1 证明拥有私钥的方法	20
3.2.2 组织机构身份的鉴别	20
3.2.3 个人身份的鉴别	21
3.2.4 没有验证的订户信息	21
3.2.6 互操作准则	21
3.3 密钥更新请求的标识与鉴别	21
3.3.1 常规密钥更新的标识与鉴别	22
3.3.2 吊销后密钥更新的标识与鉴别	22
3.4 吊销请求的标识与鉴别	22
4. 证书生命周期操作要求	22
4.1 证书申请	22
4.1.1 证书申请实体	22
4.1.2 注册过程与责任	22
4.2 证书申请处理	23
4.2.1 执行识别与鉴别功能	23
4.2.2 证书申请批准和拒绝	23
4.2.3 处理证书申请的时间	23
4.3 证书签发	23
4.3.1 证书签发中注册机构和电子认证服务机构的行 为	23
4.3.2 电子认证服务机构和注册机构对订户的通告	24
4.4 证书接受	24
4.4.1 构成接受证书的行为	24
4.4.2 电子认证服务机构对证书的发布	24
4.4.3 电子认证服务机构对其他实体的通告	24
4.5 密钥对和证书的使用	24

4.5.1	订户私钥和证书的使用	24
4.5.2	依赖方公钥和证书的使用	25
4.6	证书更新	25
4.6.1	证书更新的情形	25
4.6.2	请求证书更新的实体	25
4.6.3	证书更新请求的处理	26
4.6.4	颁发新证书时对订户的通告	26
4.6.5	构成接受更新证书的行为	26
4.6.6	电子认证服务机构对更新证书的发布	26
4.6.7	电子认证服务机构对其他实体的通告	26
4.7	证书密钥更新	26
4.7.1	证书密钥更新的情形	26
4.7.2	请求证书密钥更新的实体	26
4.7.3	证书密钥更新请求的处理	27
4.7.4	颁发新证书时对订户的通告	27
4.7.5	构成接受密钥更新证书的行为	27
4.7.6	电子认证服务机构对密钥更新证书证书的发布	27
4.7.7	电子认证服务机构对其他实体的通告	27
4.8	证书变更	27
4.8.1	证书变更的情形	27
4.8.2	请求证书变更的实体	27
4.8.3	证书变更请求的处理	28
4.8.4	颁发新证书时对订户的通告	28
4.8.5	构成接受变更证书的行为	28
4.8.6	电子认证服务机构对变更证书的发布	28
4.8.7	电子认证服务机构对其他实体的通告	28
4.9	证书吊销和挂起	28
4.9.1	证书吊销的情形	28
4.9.2	请求证书吊销的实体	30
4.9.3	吊销请求的流程	30

4.9.4	吊销请求宽限期	30
4.9.5	电子认证服务机构处理吊销请求的时限	30
4.9.6	依赖方检查证书吊销的要求	30
4.9.7	CRL 发布频率	30
4.9.8	CRL 发布的最大滞后时间	30
4.9.9	在线状态查询的可用性	31
4.9.10	在线状态查询要求	31
4.9.11	吊销信息的其他发布形式	31
4.9.12	密钥损害的特别要求	31
4.9.13	证书挂起的情形	31
4.9.14	请求证书挂起的实体	31
4.9.15	挂起请求的流程	31
4.9.16	挂起的期限限制	32
4.10	证书状态服务	32
4.10.1	操作特征	32
4.10.2	服务可用性	32
4.10.3	可选特性	32
4.11	订购结束	32
4.12	密钥生成、备份与恢复	32
4.12.1	密钥生成、备份与恢复的策略与行为	33
4.12.2	会话密钥的封装与恢复的策略与行为	33
5.	认证机构设施、管理和操作控制	33
5.1	物理控制	33
5.1.1	场地位置与建筑	33
5.1.2	物理访问	34
5.1.3	电力与空调	34
5.1.4	水患防治	35
5.1.5	火灾防护	35
5.1.6	介质存储	35
5.1.7	废物处理	35

5.1.8 异地备份	36
5.2 程序控制	36
5.2.1 可信角色	36
5.2.2 每项任务需要的人数	36
5.2.3 每个角色的识别与鉴别	37
5.2.4 需要职责分割的角色	37
5.3 人员控制	37
5.3.1 资格、经历和无过失要求	37
5.3.2 背景审查程序	38
5.3.3 培训要求	38
5.3.4 再培训周期和要求	38
5.3.5 工作岗位轮换周期和顺序	38
5.3.6 未授权行为的处罚	38
5.3.7 独立合约人的要求	38
5.3.8 提供给员工的文档	39
5.4 审计日志程序	39
5.4.1 记录事件的类型	39
5.4.2 处理日志的周期	40
5.4.3 审计日志的保存期限	40
5.4.4 审计日志的保护	40
5.4.5 审计日志备份程序	40
5.4.6 审计收集系统	41
5.4.7 对导致事件实体的通告	41
5.4.8 脆弱性评估	41
5.5 记录归档	41
5.5.1 归档记录的类型	41
5.5.2 归档记录的保存期限	41
5.5.3 归档文件的保护	41
5.5.4 归档文件的备份程序	42
5.5.5 记录时间戳要求	42

5.5.6	归档收集系统	42
5.5.7	获得和检验归档信息的程序	42
5.6	电子认证服务机构密钥更替	42
5.7	损害和灾难恢复	42
5.7.1	事故和损害处理程序	42
5.7.2	计算资源、软件和/或数据的损坏	43
5.7.3	实体私钥损害处理程序	43
5.7.4	灾难后的业务连续性能力	43
5.8	电子认证服务机构或注册机构的终止	43
6	认证系统技术安全控制	43
6.1	密钥对的生成和安装	43
6.1.1	密钥对的生成	43
6.1.2	私钥传送给订户	44
6.1.3	公钥传送给证书签发机关	44
6.1.4	电子认证服务机构公钥传送给依赖方	44
6.1.5	密钥的长度	45
6.1.6	公钥参数的生成和质量检查	45
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 (m 选 n)	45
6.2.3	私钥托管	45
6.2.4	私钥备份	45
6.2.5	私钥归档	45
6.2.6	私钥导入、导出密码模块	46
6.2.7	私钥在密码模块的存储	46
6.2.8	激活私钥的方法	46
6.2.9	解除私钥激活状态的方法	46
6.2.10	销毁私钥的方法	47
6.2.11	密码模块的评估	47

6.3	密钥对管理的其他方面	47
6.3.1	公钥归档	47
6.3.2	证书操作期和密钥对使用期限	47
6.4	激活数据	48
6.4.1	激活数据的产生和安装	48
6.4.2	激活数据的保护	48
6.4.3	激活数据的其他方面	49
6.5	计算机安全控制	49
6.5.1	特别的计算机安全技术要求	49
6.5.2	计算机安全评估	49
6.6	生命周期技术控制	49
6.6.1	系统开发控制	49
6.6.2	安全管理控制	50
6.6.3	生命期的安全控制	50
6.7	网络的安全控制	50
6.8	时间戳	50
7.	证书、证书吊销列表和在线证书状态协议	50
7.1	证书	50
7.1.1	版本号	51
7.1.2	证书扩展项	51
7.1.3	算法对象标识符	52
7.1.4	名称形式	52
7.1.5	名称限制	52
7.1.6	证书策略对象标识符	53
7.1.7	策略限制扩展项的用法	53
7.1.8	策略限定符的语法和语义	53
7.1.9	关键证书策略扩展项的处理规则	53
7.2	证书吊销列表	53
7.2.1	版本号	53
7.2.2	CRL 和 CRL 条目扩展项	53

7.3 在线证书状态协议	53
7.3.1 版本号	54
7.3.2 OCSP 扩展项	54
8. 认证机构审计和其他评估	54
8.1 评估的频率或情形	54
8.2 评估者的资质	55
8.3 评估者与被评估者之间的关系	55
8.4 评估内容	55
8.5 对问题与不足采取的措施	55
8.6 评估结果的传达与发布	56
9. 法律责任和其他业务条款	56
9.1 费用	56
9.1.1 证书签发和更新费用	56
9.1.2 证书查询费用	56
9.1.3 证书吊销或状态信息的查询费用	56
9.1.4 其他服务费用	56
9.1.5 退款策略	56
9.2 财务责任	56
9.2.1 保险范围	56
9.2.2 其他资产	57
9.2.3 对最终实体的保险或担保	57
9.3 业务信息的保密	57
9.3.1 保密信息范围	57
9.3.2 不属于保密的信息	57
9.3.3 保护保密信息的信息	57
9.4 个人隐私保密	57
9.4.1 隐私保密方案	57
9.4.2 作为隐私处理的信息	57
9.4.3 不被视为隐私的信息	58
9.4.4 保护隐私的责任	58

9.4.5 使用隐私信息的告知与同意	58
9.4.6 依法律或行政程序的信息披露	58
9.4.7 其他信息披露情形	58
9.5 知识产权	58
9.6 陈述与担保	59
9.6.1 电子认证服务机构的陈述与担保	59
9.6.2 注册机构的陈述与担保	59
9.6.3 订户的陈述与担保	59
9.6.4 依赖方的陈述与担保	60
9.6.5 其他参与者的陈述与担保	60
9.7 担保免责	60
9.8 有限责任	61
9.9 赔偿	61
9.10 有效期限与终止	62
9.10.1 有效期限	62
9.10.2 终止	62
9.10.3 效力的终止与保留	62
9.11 对参与者的个别通告与沟通	62
9.12 修订	63
9.12.1 修订程序	63
9.12.2 通知机制与期限	63
9.12.3 必须修改业务规则的情形	63
9.13 争议处理	63
9.14 管辖法律	63
9.15 与适用法律的符合性	63
9.16 一般条款	64
9.16.1 完整协议	64
9.16.2 转让	64
9.16.3 分割性	64
9.16.4 强制执行	64

9.16.5 不可抗力	64
9.17 其他条款	64

1.概括性描述

1.1 概述

浙江省数字安全证书管理有限公司(Zhejiang Digital Certificate Authority Co. Ltd., 简称 ZJCA)是依法面向社会提供电子认证服务的权威、公正的第三方机构。ZJCA 严格按照《中华人民共和国电子签名法》和《电子认证服务管理办法》的要求,以及相关管理规定,提供电子签名认证证书申请、颁发、存档、查询、废止等服务,并通过以 PKI 技术、电子签名认证证书应用技术为核心的应用安全解决方案,为电子政务、电子商务、企业信息化构建安全可靠的信任环境,为客户提供网上身份认证和信任服务等。

ZJCA 负责设立下级机构、签发用户证书、建立全省的证书和 CRL 发布服务、公布证书应用接口标准、确定体系指标、实现省内区域及行业的联接、进行基于电子签名认证证书(以下简称证书)的安全软件开发以及进行相关的业务培训等。ZJCA 可以为互联网络交易和作业双方建立信任关系,提供全面的信任和安全的服 务,保证交易和作业主体身份的真实性、信息保密性和完整性,以及交易的不可否认性,实现跨地区跨行业的互认互通,保证业务主体真正成为资源共享、公正可信的第三方。

ZJCA 采用国际国内标准的信息安全技术,建立覆盖全省并具有国际先进水平、安全可靠的、功能完善的统一信息安全电子认证服务平台;为全省电子政务、电子商务应用提供统一的身份认证机制,确保信息传输的保密性、数据交换的完整性、发送信息的不可否认性、交易者身份的确定性,实现资源共享,一证多用。

ZJCA 作为被信任的第三方,在确定真实身份后为互联网络安全电子交易和安全作业的参与方(以下称主体或实体)颁发证书。

与 ZJCA 电子认证服务相关联的实体,必须完整地理解和执行《ZJCA 电子认证业务规则》所规定的条款,承担相应的责任和业务。

《ZJCA 电子认证业务规则》作为实际应用和操作的文件依据,适用于 ZJCA、各注册机构、审核受理点、ZJCA 授权或协议的单位等实体、ZJCA 体系内的员工、申请使用证书的单位和个人等。

1.2 文档名称与标识

本文档的名称是《ZJCA 电子认证业务规则》，又称《ZJCA CPS》。

本 CPS 是 ZJCA 发布的第 5 个版本，版本号 V3.0，详细阐述了 ZJCA 在实际工作和运行中应遵循的各项规则，将通过 ZJCA 网站 (<http://www.zjca.com.cn>) 面向社会公开发布，并提供更新说明和最新版本。

ZJCA 品牌的标识为：



1.3 电子认证活动参与者

1.3.1 电子认证服务机构

电子认证服务机构 (Certificate Authority, 简称 CA) 也就是证书认证机构，是颁发证书的实体。

ZJCA 是所有下属机构和实体的根。在十分严密的保密和安全机制控制下，ZJCA 根据根证书策略，自己生成密钥对，自己签发根证书。ZJCA 根据授权和协议签发证书，ZJCA 所签发的证书与每一个证书申领实体的公钥绑定。ZJCA 已签发的在有效期内的证书，将采用证书目录服务器 LDAP (Lightweight Directory Access Protocol) 和证书黑名单服务 CRL (Certificate Revocation List) 公布该证书可以公开的信息和状态。

ZJCA 将根据业务需要，与 ZJCA 服务框架体系中未涉及的其他 CA 机构建立交叉认证关系，实现互联互通。交叉认证是指两个完全独立的、采用各自 CPS 的认证机构之间建立相互信任关系，从而使双方的证书用户可以实现互相认证。

1.3.2 注册机构

注册机构 (Registration Authority Center, 简称 RA) 也就是为最终证书申请者建立注册过程的实体，对证书申请者进行身份标识和鉴别，发起或传递证书吊销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。

浙江 RA 作为 ZJCA 授权委托的下属机构，负责对证书用户信息的审核、整理汇总、统计分析、与上级 CA 进行数据交换、管理和服务下属审核受理点。每个 RA 机构可以按照行业或行政地域设立多个审核受理点，可以直接面向最终用户提供服务。RA 机构有责任依照《中华人民共和国电子签名法》和本 CPS 妥善保存证书用户的数据，不允许将证书用户的数据透露给与证书业务无关的任何单位或个人，用作商

业利益方面的用途。

1.3.3 订户

订户，从电子认证服务机构接收证书的实体。在电子签名应用中，订户即为电子签名人。

ZJCA 证书持有者可以包括个人、单位、企业、组织、机构、服务器、网站等提供网上服务和享受网上服务的各类实体，以及其他持有 ZJCA 证书的人、物、对象或单位组织。

订户分两类：1. 被垫付的证书持有者；2. 自支付的证书持有者。

1.3.4 依赖方

依赖方，依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。

ZJCA 向依赖方保证依据本 CPS 签发证书。依赖方可在法律规定、本 CPS 和 ZJCA CP 范围内信任证书及其签名，并享有本 CPS 和 ZJCA CP 种权利。

1.3.5 其他参与者

其他参与者，如证书制造机构、证书库服务提供者、以及其他提供电子认证相关服务的实体。

ZJCA 电子认证活动的其他参与者包括以上未提及的，属于 ZJCA 认证体系的，与电子认证服务相关的其他各类实体。

1.4 证书应用

1.4.1 适合的证书应用

ZJCA 电子签名认证证书可以在电子政务公共服务、电子商务、电子办公等领域应用，为建设互联网络的信任环境开展基础性服务。证书申请者可以根据实际需要，自主判断和决定采用相应合适的证书种类。

ZJCA 可以从功能上实现以下证书应用：

订户类型	证书类型	订户私钥与证书的用途
个人	个人安全电	个人安全电子邮件证书中包含证书持有者的电子邮件地

证书	子邮件证书	址、公钥及 ZJCA 的签名。使用安全电子邮件证书的订户可以收发加密和电子签名邮件，保证订户在电子邮件传输中的机密性、完整性和不可否认性，确保电子邮件通信各方身份的真实性。
	个人身份证书	个人身份证书中包含证书持有者的个人信息、公钥及 ZJCA 的签名，在网络通讯中标识证书持有者的个人身份，可以用于个人在网上进行合同签订、定单、支付信息等活动中标明身份。
单位证书	企业或机构安全电子邮件证书	企业或机构安全电子邮件证书中包含证书持有者的电子邮件地址、公钥及 ZJCA 的签名。使用安全电子邮件证书的企业或机构可以收发加密和电子签名邮件，保证企业或机构在电子邮件传输中的机密性、完整性和不可否认性，确保电子邮件通信各方身份的真实性。
	企业或机构身份证书	企业或机构身份证书中包含企业或机构的基本信息、公钥及 ZJCA 的签名，在网络通讯中标识证书持有企业或机构的身份，可以用于企业或机构在网上业务方面的对外交易活动，如企业合同签订、网上交易等。
	部门证书	部门证书中包含部门基本信息、公钥及 ZJCA 的签名，在网络通讯中标识证书持有部门的身份，可以用于部门在网上业务方面的对外交易活动，如部门的网上交易等。
	职位证书	职位证书是用来表明证书持有者在企业中的特定职位，在网络通讯中标识证书持有者在企业中的身份，包含证书持有者的身份信息、公钥及 ZJCA 的签名，可以用于证书持有者代表企业在网上进行合同签订、定单、支付信息等活动中标明身份。
设备	应用服务器	应用服务器证书中包含应用服务器信息、公钥及 ZJCA 的

证书	证书	签名，在网络通讯中标识和验证服务器的身份。在网络应用系统中，服务器软件利用证书机制保证与其他服务器或客户端通信的安全性。
	WEB 服务器证书	WEB 服务器证书中包含服务器信息、公钥及 ZJCA 的签名，在网络通讯中标识和验证服务器的身份。在网络应用系统中，服务器软件利用证书机制保证与其他服务器或客户端通信的安全性。
	VPN 网关证书	VPN 网关证书中包含网关信息、公钥及 ZJCA 的签名，在网络通讯中标识和验证服务器的身份。在网络应用系统中，服务器软件利用证书机制保证与其他服务器或客户端通信的安全性。
	VPN 客户端证书	VPN 客户端证书中包含客户端信息、公钥及 ZJCA 的签名，在网络通讯中标识和验证服务器的身份。在网络应用系统中，服务器软件利用证书机制保证与其他服务器或客户端通信的安全性。
代码签名证书	个人代码签名证书	为独立软件开发人员提供对软件代码做电子签名的技术，可以有效防止软件代码被篡改，使用户免遭病毒与黑客程序的侵扰，同时可以保护软件开发人员的版权利益。
	企业代码签名证书	为软件开发企业提供对软件代码做电子签名的技术，可以有效防止软件代码被篡改，使用户免遭病毒与黑客程序的侵扰，同时可以保护软件开发企业的版权利益。

1.4.2 限制的证书应用

ZJCA 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订户自己承担。

其他限制的证书应用包括：

- 1.任何与国家或地方法律、法规规定相违背的应用系统；

2. ZJCA 不认可的证书应用系统。

3. 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，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

ZJCA 办公室根据《中华人民共和国电子签名法》、《电子认证服务管理办法》及其它法律法规的要求，负责本 CPS 的起草、维护和更新。ZJCA 办公室为本 CPS 的管理机构，负责起草 CPS 并根据要求提出修改报告，此外还负责此方面的对外咨询服务。

1.5.2 联系人

ZJCA 对电子认证业务规则进行严格的版本控制，并负责解释。

联系人：办公室

电话：86-571-85800770（总机）

传真：86-571-85800770-116

地址：浙江省杭州市中山北路 631 号晶晖商务大厦 22 层

邮编：310014

电子邮件：zjca@zjca.com.cn

1.5.3 决定 CPS 符合策略的机构

ZJCA 安全认证管理委员会是 ZJCA CPS 的最高决策机构，负责审核并批准 CPS。

1.5.4 CPS 批准程序

ZJCA CPS 由 ZJCA 办公室起草，ZJCA 安全认证管理委员会审核并批准。

如需进行变更，由 ZJCA 办公室提交变更报告及进行修改，ZJCA 安全认证管理委员会将对提供的变动建议进行研究分析，并征询法律顾问有关意见后，形成最终决议。ZJCA 将在决议形成后，在网站公布变更后的《ZJCA 电子认证业务规则》正式文档。

1.6 定义和缩写

电子认证服务机构 (CA): 即 **Certificate Authority**, 或 **Certifying Authority**, 是指授权签发和管理电子签名认证证书的独立可信的第三方机构, 为电子政务、电子商务的各参与方签发标识其身份的电子签名认证证书, 并对电子签名认证证书进行更新、废除等一系列管理。

注册机构 (RA): **Registration Authority**, 证书的注册机构, 负责证书的申请业务。本 CPS 指浙江省数字认证系统注册机构。

电子认证业务规则 (CPS): **Certification Practice Statement**, 是关于电子认证服务机构在全部证书服务生命周期中的业务实践 (如签发、管理、吊销、更新证书或密钥等) 所遵循的规则详细描述和声明, 提供其它业务、法律和技术方面的细节。**ZJCA CPS**, 是 **ZJCA** 证书相关业务和系统的运行规则。

证书策略 (CP), **Certification Policy** 是关于认证机构制订的一组规则, 表明证书对特定群体的适用范围, 或对不同安全需求类型的适用规则。

证书吊销列表 (CRL): **Certificate revocation list**, 认证机构的失效证书列表。证书吊销可能由于证书过期、私钥失窃或者其他原因产生。

在线证书状态协议 (OCSP): **Online Certificate Status Protocol**, **X.509** 公钥基础设施的一部分, 在不请求 **CRL** 的情况下判断证书状态的协议。

电子签名认证证书 (证书): **Certificate**, 是经一个权威的、可信赖的、公正的第三方电子认证服务机构签发的包含公开密钥拥有者信息以及公开密钥的电子文档。认证机构可以签发自己的证书, 这种自签名的证书称为该 **CA** 的根证书并用来签署下级证书。

电子签名人: 是指持有电子签名制作数据并以本人身份或者以其所代表的名义实施电子签名的实体。

电子签名依赖方: 是指基于对电子签名认证证书或者电子签名的信赖而从事有关活动的实体。

2. 信息发布与信息管理

2.1 认证信息的发布

ZJCA 通过目录服务 (**LDAP**) 发布证书状态的相关信息, 订户可以通过访问 **ZJCA**

的目录服务器获取证书的信息。ZJCA 同时提供在线证书状态查询（OCSP）和证书废除列表查询（CRL）服务。

ZJCA 系统成功签发证书后，将订户证书和 CRL 发布到目录服务器，供订户在线查询证书，并提供方便快捷的 Web 方式的证书查询服务。ZJCA 证书订户可以通过 LDAP 查询、下载并验证订户证书，同样也可以通过 OCSP 和 Web 方式验证证书有效性。

ZJCA 证书订户都可以通过 ZJCA 网站 (<http://www.zjca.com.cn>) 查询有关信息。

2.2 发布的时间或频率

ZJCA 网站提供的证书数据发布采用每 24 小时更新策略，证书废除列表（CRL）的发布策略为每 24 小时更新。

2.3 信息库访问控制

ZJCA 对外公布证书信息和 CRL 信息，任何 ZJCA 订户或非订户均可使用 LDAP 和 OCSP 方式查询证书，获取当前证书状态信息。这里的 OCSP，允许作为一种付费服务。

ZJCA 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。ZJCA 在必要时可自主选择是否实行信息的权限管理，以确保 ZJCA 相关实体的实际权益。

3. 身份标识与鉴别

3.1 命名

3.1.1 名称类型

ZJCA 生成或签发的证书命名符合 X.500 甄别名规定，遵循 X.509 标准。其通用名包含于每张证书的主题中，唯一标识证书订户的身份。各类证书命名方式不同，但是所有证书订户名都需要严格审查，命名符合 X.500 甄别名规定。

3.1.2 对名称意义化的要求

ZJCA 签发的最终订户证书所包含的名称具有通常理解的语义，用它确定证书主体中的个人、组织机构或设备的身份。

3.1.3 订户的匿名或伪名

ZJCA 订户应该使用真实名称，个人订户应使用身份证所标示的名称；单位订户应使用工商营业执照所标示的名称；设备证书应使用该设备的域名或真实的 IP 地址（当没有申请域名时）。除测试订户外，ZJCA 不接受任何匿名或者伪名，必须使用有明确意义的名称作为唯一标识符。

测试订户的 DN 项中必须包括“测试 test”。

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

ZJCA 所有证书持有者的主题甄别名，要求必须是唯一的。ZJCA 根据该主题甄别名有效的鉴别证书持有者。当出现相同的名称时，以先申请者优先使用，后申请者在唯一标识名称后面加识别码予以区别。

3.1.6 商标的识别、鉴别和角色

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 ZJCA 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，ZJCA 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

ZJCA 通过使用经电子签名的 PKCS#10 格式的证书请求，验证证书申请者拥有私钥。

3.2.2 组织机构身份的鉴别

在组织机构申请者身份的鉴别流程中，ZJCA 将按照每种证书的要求进行不同的验证。证书申请表上有申请者本身或被充分授权的证书申请者代表的签字。

ZJCA 或其注册机构、受理点等电子认证服务机构必须检查申请者所递交的身份证明文件，申请者需向 ZJCA 提供单位或服务器确实存在的有效证明，包括但不限于工商营业执照、企事业单位组织机构代码证等；申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。ZJCA 在进行法律规定的有限审查后，不承担

对申请者身份证明文件（如身份证等）进行合法性甄别的义务。

3.2.3 个人身份的鉴别

在个人申请者身份的鉴别流程中，ZJCA 可以按照每种证书相应的要求进行不同验证。证书申请表上有申请者本身或被充分授权的证书申请者代表的签字。

ZJCA 或其注册机构、受理点等电子认证服务机构必须检查申请者所递交的身份证明文件，申请者需向 ZJCA 提供单位或服务器确实存在的有效证明，包括但不限于身份证、护照等；申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。ZJCA 在进行法律规定的有限审查后，不承担对申请者身份证明文件（如身份证等）进行合法性甄别的义务。

对于包括邮寄、传真等非现场方式进行的身份鉴别，ZJCA 可要求申请者提供额外的身份鉴别资料和证明，并选择认为合理的方式辅助进行鉴别。

3.2.4 没有验证的订户信息

ZJCA 对于没有验证过的订户信息包括但不限于电话号码、邮编、地址、电子邮件等，ZJCA 将采取保密措施，但不承担由于该信息引起的任何责任和纠纷。

3.2.5 授权确认

注册机构将要求被授权人递交相应的申请者授权证明文件，并对其递交的材料作真实性声明，承担相应的法律责任。ZJCA 会按照本 CPS 的规定，对材料进行鉴别。ZJCA 也可能采取附加的或者额外的方式进行这种鉴别。

如果被授权人拒绝注册机构或 ZJCA 的身份与授权鉴别要求，那么就被视作放弃对证书的申请。同时 ZJCA 声明，ZJCA 和注册机构可以拒绝任何申请请求，并且没有对此说明原因的义务。

3.2.6 互操作准则

无规定。

3.3 密钥更新请求的标识与鉴别

通常订户的密钥存在有效期，ZJCA 可以决定该有效期的长短。密钥到期后必须更新（重新产生一组公钥和私钥密钥对），并向发证机构申请重新签发证书。

当订户与证书相关的信息发生变化或者对密钥的安全有顾虑时，必须重新注册、产生新的密钥对，并向发证机构申请重新签发证书。为了风险管理和安全考虑，重

新申请签发证书时，订户将不被允许使用旧的密钥对，除非订户愿意书面表示自己承担由此产生的一切责任和后果。

当国家主管部门对密钥的管理、更新等有规定的，ZJCA 将严格予以执行。

3.3.1 常规密钥更新的标识与鉴别

证书有效期结束后的常规密钥更新的识别与鉴别，参见本 CPS 3.2 初始身份确认。

3.3.2 吊销后密钥更新的标识与鉴别

证书吊销后的常规密钥更新的识别与鉴别，参见本 CPS 3.2 初始身份确认。

3.4 吊销请求的标识与鉴别

参见本 CPS 3.2。

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

任何合法的组织机构和自然人以及有明确身份归属的其他网络主体均可申请证书，以保证网络作业的安全和可靠。

设备证书可由设备拥有机构、个人或被授权使用该设备的实体申请；代码签名证书由软件开发者或被授权实体申请。

4.1.2 注册过程与责任

4.1.2.1 注册过程

1. 证书申请者携带相关证明到 ZJCA，填写相关申请表格，签署订户协议。
2. 受理机构审核证书申请者和相关身份资料的真实性。如果身份鉴别未通过，受理机构将拒绝为用户发放证书。
3. 如果身份鉴别通过，受理机构录入信息、审核证书申请信息，提交 CA 处理。
4. CA 根据证书请求签发证书。
5. 受理机构下载证书后，将其递交给申请者。

4.1.2.2 各方责任

1. 最终订户

最终订户须明确表示其愿意接受相关的订户协议中所规定的相关责任与义务，并需要提供真实、准确的申请信息。

2. 认证机构

认证机构必须设定安全可靠的证书申领方式与程序，注册过程必须做到：

- 提供必需的信息。
- 保证订户信息不被篡改、私密信息不被泄露。
- 注册过程必须保证订户明确同意相关的订户协议，才能完成注册过程。
- 按本 CPS3.2.1 产生一个密钥对，并将公钥传给注册机构，认证机构。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

当认证机构、注册机构接收到订户的证书申请后，参见本 CPS3.2 的要求，对订户进行身份识别与鉴别。

4.2.2 证书申请批准和拒绝

注册机构对证书申请者提交的申请信息及身份信息进行鉴别，鉴别其是否完整、真实、有效。经鉴别符合要求后，将批准申请。如果申请者未能通过审核，注册机构将拒绝申请者的申请，并以适当的方式，在合适的时间内通知申请者。

4.2.3 处理证书申请的时间

注册机构将在接受用户申请 5 个工作日内对证书申领者提交的信息进行鉴别和审核，并作出批准或者拒绝的决定。

4.3 证书签发

4.3.1 证书签发中注册机构和电子认证服务机构的行为

在证书的签发过程中注册机构的管理员负责证书申请的审批，并通过操作注册机构系统将签发证书的请求发往 ZJCA 的证书签发系统。注册机构发往 ZJCA 的证书签发请求信息须有注册机构的身份鉴别与信息保密措施，并确保请求发到正确的 ZJCA 证书签发系统。

ZJCA 的证书签发系统在获得注册机构的证书签发请求后，对来自注册机构的信

息进行鉴别与解密，对于有效的证书签发请求，证书签发系统签发证书。

4.3.2 电子认证服务机构和注册机构对订户的通告

无论是拒绝还是批准申请者的证书申请，注册机构须通过适当的方式通知申请者。如果证书申请获得批准并签发，注册机构应通过适当的方式告诉申请者如何获取证书。

ZJCA 的证书签发系统签发证书后，将证书签发的信息通过适当的方式通知注册机构。

4.4 证书接受

4.4.1 构成接受证书的行为

当申请者填写证书申请表，并提供真实、准确的身份信息经注册机构审核通过，同意相关订户协议后，并接受了载有证书的介质后即视为申请者已经接受此证书。

如申请者对证书有异议，应在 5 个工作日之内提出。

4.4.2 电子认证服务机构对证书的发布

ZJCA 在签发证书后定期将该证书发布到目录系统上，并通过安全的机制向依赖方提供查询服务。

4.4.3 电子认证服务机构对其他实体的通告

ZJCA 不需要通知其他实体证书的签发。

4.5 密钥对和证书的使用

密钥对和证书须用于其规定的、批准的用途。签名密钥对用于签名与签名验证，加密密钥用于加密解密。

密钥对和证书不应用于其规定的、批准的用途之外的目的，否则其应用是不受保障的。

4.5.1 订户私钥和证书的使用

订户在使用私钥和证书时须遵循以下约定：

1. 订户只能在规定的范围内使用私钥和证书，参见本 CPS1.4，并对使用行为承担责任；
2. 订户在使用证书时必须遵守相关的订户协议及本 CPS 和 ZJCA CP 的要求；

3. 订户应当妥善保存其私钥和证书，避免遗失、泄露、被篡改或者被盗用,避免他人未经授权而使用证书的情形发生。任何人使用证书时都必须检验证书的有效性。

4.5.2 依赖方公钥和证书的使用

在依赖方接受电子签名信息后需要：

1. 获得电子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. 证书的用途适用于对应的签名；
4. 使用证书上的公钥验证签名；
5. 确认电子签名对应的证书状态正常，没有进入 CRL 列表。

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受方时，须先通过适当的途径获得接受方的加密证书，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受方。

4.6 证书更新

证书更新指在证书有效期，ZJCA 在不改变证书中订户的公钥情况下，为 ZJCA 订户签发一张新证书。

为保证证书及其密钥对的安全有效，ZJCA 会为签发的证书设置有效期，这是为了保证订户的权利。如果订户需要更新证书，必须在证书有效期到期前到注册机构办理。

4.6.1 证书更新的情形

当订户的证书有效期到期前，ZJCA 将作出合理的努力，在证书有效期满之前向证书订户或者证书申请受托人、垫付商或者代理商发送证书更新提示；合理的努力包括但不限于网站提示、系统提示、书面提示、E-mail 通知或者其它方式，但 ZJCA 采取了上述任意一项提示或者通知方式，均可被视作进行了合理的努力。

当订户证书的密钥丢失或损坏时，也可申请证书更新。

4.6.2 请求证书更新的实体

订户可向 ZJCA 申请更新持有的证书。包括：由 ZJCA 颁发的原有证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的

各种实体，以及其他凡是 ZJCA 各类证书（包括测试证书）的有效期限未到的证书持有者。

4.6.3 证书更新请求的处理

处理证书更新请求的过程，包括申请鉴别、签发证书。对申请的鉴别须基于以下几个方面：

申请对应的原证书存在并且由 ZJCA 签发。

基于原注册信息进行身份鉴别。

在以上鉴别通过后才可签发证书。

4.6.4 颁发新证书时对订户的通告

参见本 CPS4.3.2。

4.6.5 构成接受更新证书的行为

参见本 CPS4.4.1。

4.6.6 电子认证服务机构对更新证书的发布

参见本 CPS4.4.2。

4.6.7 电子认证服务机构对其他实体的通告

参见本 CPS4.4.3。

4.7 证书密钥更新

证书密钥更新是指订户需要生成新密钥并申请为新密钥签发新证书。

4.7.1 证书密钥更新的情形

如果出现下列情形，订户必须选择证书密钥更新或者重新申请证书：

1. 证书到期并且密钥对的试用期也到期；
2. 证书密钥对已经被泄露、被窃取、被篡改或者其它原因导致的密钥对安全性无法得到保证；
3. 证书被吊销后需要重新获得证书。

4.7.2 请求证书密钥更新的实体

个人证书由订户提出申请；单位证书由企业、组织机构授权的人员提出申请；设备证书由域名或者 IP 地址的所有者提出申请；代码签名证书由发行商提出申请。

4.7.3 证书密钥更新请求的处理

在证书到期之后，订户只能向注册机构提交密钥更新申请进行密钥更新。处理密钥更新请求的过程，包括申请鉴别、签发证书。对申请的鉴别须基于以下几个方面：

申请对应的原证书存在并且由 ZJCA 签发。

基于原注册信息进行身份鉴别。

在以上鉴别通过后才可签发证书。

4.7.4 颁发新证书时对订户的通告

参见本 CPS4.3.2。

4.7.5 构成接受密钥更新证书的行为

参见本 CPS4.4.1。

4.7.6 电子认证服务机构对密钥更新证书证书的发布

参见本 CPS4.4.2。

4.7.7 电子认证服务机构对其他实体的通告

参见本 CPS4.4.3。

4.8 证书变更

在证书有效期内，当证书信息发生变化，订户或者其它参与者可以选择证书变更，申请签发新的证书。

4.8.1 证书变更的情形

改变证书中除订户公钥之外的信息而签发新证书的情形：订户提供的证书变更信息不涉及证书的主题甄别名等关键信息。

改变订户公钥的信息而签发新证书的情形：订户提供的证书变更信息涉及证书的主题甄别名等关键信息。

4.8.2 请求证书变更的实体

ZJCA 颁发的原有证书的个人、单位、服务器设备、企业、组织、网站等提供网上服务和享受网上服务的各种实体，以及其他凡是 ZJCA 各类证书（包括测试证书）的证书持有者均可向 ZJCA 申请变更自己持有的证书。

4.8.3 证书变更请求的处理

订户在申请证书变更时，由注册机构根据申请变更的证书种类，提供相应的表格，订户填写完表格后；注册机构根据表格进行证书变更注册等制作工作。

订户在申请办理证书变更时，有责任在证书申请中提供准确有效的信息，提供相关的证明文件。

4.8.4 颁发新证书时对订户的通告

参见本 CPS4.3.2。

4.8.5 构成接受变更证书的行为

参见本 CPS4.4.1。

4.8.6 电子认证服务机构对变更证书的发布

参见本 CPS4.4.2。

4.8.7 电子认证服务机构对其他实体的通告

参见本 CPS4.4.3。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

a) 证书有效期内，如果出现下列情况（包括但不限于下列情况），ZJCA 可以直接将证书予以吊销：

1. 由于证书管理系统的不适用或者证书系统的整合需要；
2. 由于证书订户未能履行与 ZJCA 之间的协议（如未缴纳费用等）而被这些有权力主张吊销的实体提出；
3. 由于证书的不当使用而违反国家的法律法规、本 CPS 或 ZJCA CP 规定的主要和重要义务；
4. 政府主管机构或者法院依照正式合法的程序提出申请；
5. 订户（或其授权的代理人）请求吊销证书，一旦确定请求吊销者是订户本人的；
6. 订户申请证书服务时，提供不真实或者欺骗性材料的；
7. ZJCA 因运营问题，导致 ZJCA 内部重要数据或 ZJCA 根密钥失密等原因的；
8. 证书的私钥丢失、被盗、被篡改、被未经授权泄露或被损害；

9. 发现并证明某证书没有根据本 CPS 或 ZJCA CP 要求的程序而签发；

10. 如果确认下级发证机构有任何一种下述行为，无论下级发证机构是否同意，ZJCA 将做出合理努力来吊销下级发证机构的证书：ZJCA 知道或有合理理由认为下级发证机构证书中陈述的某些关键事实是虚假的、签发证书的某些关键条件即未得到满足也未放弃、下级发证机构的私钥或可信系统存在安全风险并在本质上影响到其证书的可信度、下级发证机构已经违背了本 CPS 或 ZJCA CP 规定的重要职责。

11. 由于不可抗力、自然灾害、计算机或通信故障、法律法规的修改、政府行为（包括但不限于出口控制管理部门的限制行为）或其它超出人力合理控制的原因，造成其它人的信息受到严重威胁或危及其安全，从而拖延或阻止了订户责任的执行。

b) 证书在有效期内，如果出现下列情况，订户必须提出吊销请求：

1. 与证书中的公钥相对应的私钥被泄密、被窃取、被篡改或者其它原因产生对私钥的安全性顾虑；

2. 证书中的订户相关信息发生变更；

3. 由于证书不再需要用于原来的用途而要求终止；

4. 证书中的相关内容和提交申请进行注册时不一致；

5. 证书持有者已经不能履行或违反了本 CPS 或 ZJCA CP 或其它协议、法规及法律所规定的责任和义务。

c) 下级子 CA 证书在有效期内，如果出现下列情况，下级发证机构必须提出吊销请求，ZJCA 必须迅速把任何该类吊销的情况通知给下级注册机构：

1. 下级注册机构证书中相关内容发生变化的；

2. 与证书中的公钥相对应的私钥被泄密、被窃取、被篡改或者其它原因产生对私钥的安全性顾虑；

3. 证书中的相关内容和提交申请进行注册时不同的，或者违反了本 CPS 或 ZJCA CP 或其他协议、法规及法律所规定的责任和义务的；

4. 因为业务发展、财务、法律法规或者其它不可抗因素，不得不终止服务结束运营的；

5. 其它 ZJCA 认为可以进行吊销的理由。

d) 其它 ZJCA 认为可以进行吊销的理由。

e) ZJCA 没有义务一定要公开某一张证书被吊销的原因。

4.9.2 请求证书吊销的实体

在符合本 CPS4.9.1 所述的情形下，请求证书吊销的实体与本 CPS4.1.1 证书申请实体相同。

另外，ZJCA 也可以在本 CPS4.9.1 所述的情形下主动吊销订户的证书。

4.9.3 吊销请求的流程

最终订户吊销证书时可按以下流程进行：

订户（或其授权委托人）填写书面申请表并签名或盖章，同时提交相应的证明材料，向注册机构或关联过新应用的注册机构提出吊销证书请求。

ZJCA、注册机构在接到最终订户的吊销请求后，需通过可靠的方式确认请求确实来自最终订户。

4.9.4 吊销请求宽限期

订户一旦发现需要吊销证书，应在 8 小时之内向发放该证书的注册机构或关联过新应用的注册机构提出吊销请求。

4.9.5 电子认证服务机构处理吊销请求的时限

ZJCA 或其授权的证书注册机构从收到吊销请求到审核完成，做出吊销决定并将吊销证书发布到信息库，全部工作应当在 24 小时内完成。订户正式提出证书吊销申请后因使用该证书造成的损失，ZJCA 不予承担。

说明：订户在正式提出证书吊销申请后不得在交易中继续使用此证书，否则由此产生的后果，由订户自行承担。

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 ZJCA 发布的 CRL 完成。

4.9.7 CRL 发布频率

CRL 发布频率为 24 小时一次，在发布的同时对原有内容进行更新。

4.9.8 CRL 发布的最大滞后时间

ZJCA 在生成 CRL 的 24 小时后会更新信息库。

4.9.9 在线状态查询的可用性

ZJCA 须提供证书状态的在线查询服务 (OCSP)，以供安全保障要求高的应用使用。

4.9.10 在线状态查询要求

对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，依赖方在信赖一个证书前必须通过证书状态在线查询检查该证书的状态。

4.9.11 吊销信息的其他发布形式

除了 CRL、OCSP 外，ZJCA 可以提供其他形式的吊销信息发布，但这不是必须的。

4.9.12 密钥损害的特别要求

当订户发现、或有充足的理由发现其密钥遭受安全威胁时，应及时地提出证书吊销请求。

4.9.13 证书挂起的情形

当证书仍处于有效期，为了保留订户的证书使用权利，而不申请吊销该证书，当出现下列情况时，可以进行证书挂起：

1. 证书订户要求暂停使用该证书一段时间；
2. 订户未能履行与 ZJCA 签订的协议中应尽的义务，但向 ZJCA 提出申请并获得批准后；
3. 除证书订户（或者其授权的委托代理人）外的其它实体，如电子认证服务机构及其授权的服务机构、法院、政府主管部门及其他公共权利部门，向 ZJCA 提出挂起证书请求并获得批准。

4.9.14 请求证书挂起的实体

只有证书订户本人或者其授权的委托代理人，以及电子认证服务机构及其授权的服务机构、法院、政府主管部门及其他有关部门等，才有权力提出证书挂起的请求。

4.9.15 挂起请求的流程

订户在申请证书挂起时，由 ZJCA 受理点根据申请变更的证书种类，发放相应的申请表，订户填写完后依据申请表按时缴纳相应的费用；受理点根据申请表进行

证书挂起注册等制作工作。订户在申请办理电子认证证书挂起时，有责任在证书申请中提供准确有效的信息，提供相关的证明文件，并按时缴纳相应费用。除证书订户以外的其它实体，如 ZJCA 的授权机构、政府公共权力部门等，提出证书挂起请求，也需按规定填写申请表并提交证明材料。ZJCA 审核通过挂起请求后，应在 24 小时内办理挂起操作。强制挂起的订户证书，需在 3 个工作日内通过电子邮件、传真或邮寄等方式通知订户。

4.9.16 挂起的期限限制

证书挂起的最长时间是 6 个月，如果没有接到订户的挂起或其他申请，该证书将被废除。如证书挂起时间内到达有效期，ZJCA 也将废除该证书。

4.10 证书状态服务

4.10.1 操作特征

ZJCA 订户可以通过 OCSP 方式、LDAP 方式在线查询证书状态。

以下为各发布点的地址：

OCSP: 211.90.237.6

LDAP: zjca.com.cn:389

4.10.2 服务可用性

ZJCA 提供 7×24 小时 OCSP 方式、LDAP 方式查询服务。

4.10.3 可选特性

无规定

4.11 订购结束

以下二种情形将被视为订购结束：

证书到期后即视为订购结束。

证书吊销视为订购结束。

4.12 密钥生成、备份与恢复

ZJCA 制订了严格的管理流程，从技术与制度上保证了在生成证书时，与此张证书相对应的私钥在存储介质中生成且只留存在存储介质中，不会留存任何备份。

4.12.1 密钥生成、备份与恢复的策略与行为

订户加密证书密钥对可以由 ZJCA 的密钥管理中心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：

- 1) 证书持有人提出申请；
- 2) 注册机构提出申请，并有充分的理由；
- 3) 国家执法、司法机构因执法、司法的需要；
- 4) 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，ZJCA 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

ZJCA 认证机构的物理场地满足以下安全要求并最有效地控制风险：

防止物理非法进入 4 层物理结构及完善的安全管理体系保护 ZJCA 的运营设施和信息安全。

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 ZJCA 认证机构内的受到限制区域。

维护 CA 服务的完整性、可用性。针对环境的安全威胁，采用了一些有力的措施，例如 UPS 电源保障、数据线路、门禁系统、监控装置和屏蔽机房的建设等。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。

5.1.1 场地位置与建筑

ZJCA 认证业务的运营场地是按照国家相关部门制定的《电子计算机机房设计规范》(GB 50174-93)、《计算站场地技术条件》(GB 2887-89)、《计算站场地安全要求》(GB 9361-88)、《低压配电装置及线路设计规范》(GB 5054-95)、《采暖通风与空气调节设计规范》(GBJ 19-87)、《建筑防雷设计规范》(GB 157)、《工业企业通信接地

设计规范》(GBJ 79-85)、《工业企业照明设计标准》(GB 50034-1992) 等物理场地建设规范进行构建的, 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。敏感区域及以上区域的墙壁, 在其双层干饰面内墙之间, 采用镀钢夹层。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。

物理安全是基于物理层级的保护, 每一物理层就是一个屏障, 需要设置可以控制进出的门禁系统来控制每个人进出每一个区域。每一层区域必须有非常严格的控制方法防止未经授权的物理访问。而且要求每一个物理安全层在物理上必须能完全包含下一个物理安全层, 最外层的安全层应该是整个建筑物的外墙。

5.1.2 物理访问

ZJCA 的物理设施的访问控制系统是与控制各层门进出的门禁系统相结合的, 并实现了以下安全功能:

- 进出每一道门都有记录作为审计依据;
- 每道门的进出采用身份识别卡或生物识别鉴定的控制方法;
- 授权人员进出每一道门都会有时间记录和相关信息提示;
- 关键区域的门都设有强行开门报警;
- 整套访问控制系统配有断电保护装置提供紧急用电;
- 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

ZJCA 有安全、可靠的电力供电系统及电力备用系统, 以确保系统 7×24 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。另外, ZJCA 认证机构还具有空调系统控制运营设施中的温度和湿度。

1、本系统建设的供配电系统达到以下效果: 完全根据各设备电负荷的大小, 选用相应线径的供电电缆和不同容量的电源滤波器。多处采用低泄漏电流的电源滤波器, 达到插入衰减能力与屏蔽室综合效能一致的效果。针对大容量的供电全部采取三相供电方式。对于室内电缆沟或管线走线, 按照实际要求位路配路电源插座。

2、根据《机房建设概算》和 GB50174-93《电子计算机机房设计规范》的有关

规定，ZJCA 的机房使用独立的空调与冷却系统，机房的温湿度控制执行 B 级标准，即温度为 $23^{\circ}\text{C} \pm 5^{\circ}\text{C}$ ，相对湿度为 $55\% \pm 15\%$ ，空气洁净度为粒径 $\geq 0.5\mu\text{m}$ ，个数 $\leq 18000/\text{dm}^3$ 。通过设备照明、通风、人体体温及建筑热量的估算，24 小时稳定控制室温湿度。

5.1.4 水患防治

ZJCA 数据中心有专门的技术措施，防止漏水的出现，并能够在出现漏水时最大程度地减小漏水对认证系统的影响

5.1.5 火灾防护

5.1.5.1 结构防火

ZJCA 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，防护方法应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

ZJCA 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。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

ZJCA 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

当 ZJCA 电子认证服务系统使用的硬件设备、存储设备、加密设备等废弃不用时，将按国家的有关规定进行报废处理，其中所涉及敏感性、机密性信息都将被安

全、彻底的消除，保证其信息无法被恢复与读取。

当电子认证服务机构保存的相关数据已不再需要或存档的期限已满时，ZJCA 将完全销毁这些数据。

所有处理行为将由至少 2 名人员同时进行，相互监督，并将处理行为记录在案，并签字确认，以供审查的需要，所有销毁行为遵守我国的法律。

5.1.8 异地备份

ZJCA 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 ZJCA 建筑物以外的安全的地方。

5.2 程序控制

5.2.1 可信角色

ZJCA 的可信人员包括：

鉴证和客户服务人员

安全管理人员

密钥与密码设备管理人员

加密设备操作人员

系统管理员

人力资源管理人员

掌握 CA 秘密共享的人员。

能够进入三层以上工作区域的人员。

5.2.2 每项任务需要的人数

ZJCA 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。

鉴证和签发证书，要求 2 个可信人员的参与。

访问 CA 密钥离线生成室和 CA 密钥离线存放室，至少两名有访问权限的人员。

掌管秘密共享，至少 5 人。

操作存放有 CA 密钥的密码设备，包括密钥生成、分配、备份、销毁等，至少需要 3 个秘密共享持有人，一个密钥管理员，一个见证人。

5.2.3 每个角色的识别与鉴别

对于物理访问控制，ZJCA 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 ZJCA 及注册机构证书管理员，需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，需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。ZJCA 对如下人员进行了职责分割：

密钥管理员

安全管理员

证书申请鉴证人员

系统维护人员

秘密分割持有者

5.3 人员控制

5.3.1 资格、经历和无过失要求

在 ZJCA 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。

ZJCA 客户服务人员必须受过专门的客户服务技能培训，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 ZJCA 负责。

ZJCA 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 ZJCA 安全要求，熟悉 ZJCA 安全与审计指南，有很强的责任感。为了达到此要求，ZJCA 将对安全管理人员进行培训。

ZJCA 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。

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

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，ZJCA 将对雇佣的人员先进行背景调查。在成为 ZJCA 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。

ZJCA 依据有关材料进行背景调查，在调查过程中，ZJCA 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，ZJCA 将拒绝可信职位候选人获得有关职位或取消其可信人员的资格。

5.3.3 培训要求

为了使有关人员能胜任其承担的工作，ZJCA 对所有入职员工制定有专门的培训计划，培训内容包括：

本人工作职责。

安全管理要求及制度。

事故和安全威胁的报告和处理。

对于销售、服务和支持还包括

PKI 及应用。

ZJCA 的产品与服务。

客户服务流程与要求（客户服务）。

安全操作流程（系统、密钥）。

5.3.4 再培训周期和要求

ZJCA 根据业务需要安排。

5.3.5 工作岗位轮换周期和顺序

内部安排。

5.3.6 未授权行为的处罚

ZJCA 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

在有限制的情况下，独立合约人或顾问可以担任可信职位。任何合约人或顾问在某一职务的职能和安全标准应与相应职位的内部雇员一样。

担任可信角色的独立合约人和顾问需要通过本 CPS5.3.2 中所述的背景调查程序，否则，他们不能担任可信角色，当进入敏感区时，只能在认证机构人员的陪同和直接监督下访问认证机构的安全设施，完成有关的工作。

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，这些资料通常是不公开的。

5.4 审计日志程序

5.4.1 记录事件的类型

ZJCA 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、卸载和弃用。

这些记录都是密钥管理员完成的纸质或电子记录。

➤ 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。
- 对于系统文件的非授权的访问及访问企图。
- 安全、敏感的文件或记录的读、写或删除。
- 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。

这些记录由操作系统自动完成，ZJCA 的系统维护人员会定期检查系统日志。

➤ 系统操作事件，包括：

- 系统启动和关闭。
- 系统权限的创建、删除、设置或修改密码。

这些记录由操作系统自动完成，ZJCA 的系统维护人员会定期检查系统日志。

➤ ZJCA 物理设施的访问

- 授权人员进出。
- 非授权人员进出及陪同人。
- 安全存储设施（离线密钥）的访问。

授权人员进出物理设施由 ZJCA 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：

- 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 CA 和订户证书生命周期内的管理事件日志，ZJCA 将一个季度进行一次内部检查、审计。

系统安全事件和系统操作事件日志 ZJCA 将每周进行一次检查、处理。

ZJCA 物理设施的访问日志 ZJCA 将每月进行一次检查、处理。

5.4.3 审计日志的保存期限

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

ZJCA 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、删除或以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，ZJCA 定期进行备份。

5.4.6 审计收集系统

对于电子审计信息，ZJCA 设置了专门的审计信息存储系统，自动或人工完成审计信息的收集。对于纸质的审计信息，则有专门的文件管理柜来实现审计信息的收集。

5.4.7 对导致事件实体的通告

当审计记录报告一个事件时，ZJCA 会立即通知引起该事件的个人、组织机构。

5.4.8 脆弱性评估

根据审计记录，ZJCA 定期进行系统、物理场地、运营管理、人事管理等方面的安全脆弱性评估，并根据评估报告采取措施。

5.5 记录归档

5.5.1 归档记录的类型

ZJCA 归档下列信息：

审计记录的归档依据本 CPS5.4.1 要求

证书申请信息

证书签发过程中的支持文档

证书生命周期的相关信息

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，保留一年以上。

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。

5.5.3 归档文件的保护

ZJCA 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

ZJCA 对归档文件定期进行备份，分为增量备份和全备份。增量备份每天进行，全备份每周进行。备份文件将被放在异地进行保存。

5.5.5 记录时间戳要求

ZJCA 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或采用时间戳技术。

5.5.6 归档收集系统

ZJCA 有专门的电子归档文档的存放系统。

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验证。

5.6 电子认证服务机构密钥更替

当 CA 密钥对的累计寿命超过本 CPS 6.3.2 中规定的最大生命期，ZJCA 将启动密钥更新流程，替换已经过期的 CA 密钥对。ZJCA 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（或最终订户）的证书请求，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 损害和灾难恢复

5.7.1 事故和损害处理程序

ZJCA 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

- 网络与信息系统应急方案
- 安全事故应急处理方案等。

5.7.2 计算资源、软件和/或数据的损坏

ZJCA 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

对于实体私钥的损害，ZJCA 有如下处理要求和程序：

1) 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，并立即通过电话的方式通知 ZJCA 或注册机构吊销其证书。

2) 当 ZJCA 或注册机构发现证书订户的实体私钥受到损害时，ZJCA 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。发布证书吊销信息。

3) 当 ZJCA 或注册机构的 CA 证书出现私钥损害时，ZJCA 将立即吊销 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 灾难后的业务连续性能力

ZJCA 异地保存了系统数据备份系统，在物理场地或系统数据出现重大灾难时，能够根据需要尽快恢复其业务。

5.8 电子认证服务机构或注册机构的终止

当 ZJCA 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 认证系统技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

6.1.1.1 CA 密钥对的产生

对于 ZJCA 密钥对，ZJCA 专门的密钥管理员及若干名接受过相关培训的可信雇

员在 ZJCA 安全设施中的密钥生成室,按照 ZJCA 的密钥管理策略中规定的密钥生成规程进行产生。ZJCA 的密钥生成规程规定了 CA 密钥产生的流程控制及参加人员。ZJCA 的密钥对采用硬件实现,所使用的生成及保存的密码模块(含密钥生成算法芯片)符合国家密码主管部门的要求,并通过国家密码主管部门的鉴定。

6.1.1.2 最终订户密钥对的产生

(除服务器证书外)必须使用硬件密码模块生成密钥。对于服务器证书,订户利用 Web 服务器软件提供的密钥生成功能生成密钥或用专门的硬件加密模块。

6.1.2 私钥传送给订户

如果认证机构或注册机构在硬件加密设备中为最终订户生成密钥对,那么,它应该通过安全的、采用了防篡改封装的方式将密钥对分发给最终订户。认证机构或注册机构应记录密钥对的分发。

6.1.3 公钥传送给证书签发机关

需要 ZJCA 认证的证书公钥,最终订户通过 PKCS#10 格式的证书签名请求信息文件包格式,以电子的方式将公钥提交给认证机构(或通过注册机构),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 电子认证服务机构公钥传送给依赖方

对于 ZJCA 的主 CA 公钥,通过如下方式之一传输给依赖方:

- 1) 依赖方访问 ZJCA 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;
- 2) 依赖方访问 ZJCA 的目录系统;
- 3) ZJCA、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;
- 4) ZJCA、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;
- 5) ZJCA、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 ZJCA 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 ZJCA 通过 PKCS#7 格式将除根证书外的证书链传递给最终订户。

6.1.5 密钥的长度

ZJCA 和最终订户密钥对至少是 1024 位 RSA。

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

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

6.2 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

ZJCA 使用国家密码管理部门认可、批准的硬件密码模块生成主 CA、证书签发 CA 和其他 CA 密钥对,存储 CA 私钥。

ZJCA 制定有专门密码管理策略,在从运送、验收、初始化、离线存放、在线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。CA 密码设备的操作遵从多人在场、多人控制的原则。

6.2.2 私钥多人控制 (m 选 n)

ZJCA 的各类 CA 私钥存放在硬件加密卡中,该加密卡启动的秘密被分割保存在 5 张 IC 卡中(称为秘密共享),这 5 张 IC 卡由 ZJCA5 名可信雇员持有(称为秘密分管者),保存 ZJCA 内部保险盒中。当要操作使用 CA 私钥时(离线),需要 3 名秘密分管者持有秘密共享 IC 卡才能启动加密卡。

6.2.3 私钥托管

ZJCA 所有 CA(包括主 CA 和运营 CA)的私钥均未托管。

6.2.4 私钥备份

ZJCA 对 CA 私钥通过专门的备份加密卡进行备份,这些备份分别作为本地常规备份和异地灾难恢复备份。

6.2.5 私钥归档

当 ZJCA 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 密钥对保存在本 CP 6.2.1 所述的硬件密码模块中, 并且 ZJCA 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, ZJCA 将对其进行销毁。

6.2.6 私钥导入、导出密码模块

ZJCA 的 CA 密钥对在硬件密码模块上生成, 保存和使用。此外, 为了常规恢复和灾难恢复, ZJCA 对 CA 密钥进行复制。当 CA 密钥对从一个硬件密码模块复制到另一个硬件密码模块上时, 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 ZJCA 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、被窃、修改、非授权的泄露、非授权的使用。

6.2.7 私钥在密码模块的存储

ZJCA 私钥以加密的形式存放在硬件密码模块中, 在密码模块中使用。

6.2.8 激活私钥的方法

6.2.8.1 用户证书私钥

对于 ZJCA 签发的证书, 建议订户使用 USB-Key 等硬件密码设备存放私钥, 私钥不能出设备, 并且订户要使用 PIN 码 (口令) 机制保护私钥。要激活私钥, 用户计算机上需安装相应的驱动程序, 并输入相应 USB-Key 的 PIN 码 (口令), 私钥才激活可以使用。

6.2.8.2 服务器证书

对于 ZJCA 签发的服务器证书, 如果没有使用硬件密码模块产生、保存私钥, 则私钥是存放在服务程序的软件密码模块中, 这时订户应该使用口令对私钥进行保护。当服务程序启动, 软件加密模块被加载, 并输入相应的私钥保护口令后, 证书私钥被激活。如果使用硬件密码模块, 则私钥需要被口令保护。当硬件密码模块被安装到订户服务器上, 服务程序启动, 并输入相应私钥保护口令后, 证书私钥被激活。

6.2.9 解除私钥激活状态的方法

对于 ZJCA 的 CA 私钥, 当存放私钥的硬件密码模块断电, 私钥进入非激活状态。

6.2.10 销毁私钥的方法

私钥不再使用、不需要保存时，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授权使用。

对于 ZJCA 签发的最终订户加密证书私钥，在其生命周期结束后，订户应该妥善保存一定期限，以便于解开加密信息。对于 ZJCA 签发的最终订户签名私钥，在其生命周期结束后，无需再保存，可以通过私钥的删除、系统或密码模块的初始化来销毁。

在 ZJCA 的 CA 私钥生命周期结束后，ZJCA 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。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。

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 和最终订户证书，ZJCA 将进行归档，归档的证书存放在指定数据库中。

6.3.2 证书操作期和密钥对使用期限

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电子签名，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，直到私钥受到损害或密钥对存在被破解的风险，如加密算法被破解。当私钥受到损害或密钥对存在被破解的风险后，签名证书的公钥在技术上仍然可以用于验证数字签名，但这种验证在法律上不一定是有效的。

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

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。

另外无论是订户证书还是 CA 证书，有效期到期前，在保证安全的情况下，允许证书进行更新而密钥对不变。但是密钥对不能无限期使用。对于不同的证书，密钥对通过证书更新允许的最长使用期限如下：

- 对于根证书，其密钥对的最长允许使用年限是 50 年。
- 对于主 CA 证书，其密钥对的最长允许使用年限是 30 年。
- 对于其他 CA 证书，其密钥对的最长允许使用年限是 15 年。
- 对于最终订户证书，其密钥对的最长允许使用年限是 5 年。

6.4 激活数据

6.4.1 激活数据的产生和安装

存放有 ZJCA 的 CA 私钥的设备的激活信息（秘密共享），其产生按 ZJCA 密钥生成规程中的规定进行。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。

ZJCA 的 CA 私钥的激活数据由硬件设备内部产生，并分割保存在 5 个 IC 卡中，需通过专门的读卡设备和软件读取。

如果订户证书、管理员证书、或 RA 证书的私钥的激活数据是口令，这些口令必须：

- 由用户产生；
- 至少 6 位字符或数字；
- 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。

6.4.2 激活数据的保护

保存有 ZJCA 的 CA 私钥的激活数据的 5 个 IC 卡，由 ZJCA5 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分管者责任。秘密共享必须存放在保险盒中。

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。

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 ZJCA 的 CA 私钥的激活数据的 IC 卡，通常保存在 ZJCA 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 ZJCA 安全管理人员和密钥管理人员的监督下进行。

当订户证书私钥的激活数据需要进行传送时，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。

6.4.3.2 激活数据的销毁

存有 ZJCA 的 CA 私钥的激活数据的 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 ZJCA 安全管理人员和密钥管理人员的监督下进行。

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

ZJCA 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，认证机构只允许有工作需求的必要人员访问产品服务器，一般的应用用户在产品服务器上没有账户。

认证机构的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，只有认证机构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直接访问认证系统数据库。

6.5.2 计算机安全评估

ZJCA 的 CA 系统及其运营环境符合国家密码管理局的安全保障要求。

6.6 生命周期技术控制

6.6.1 系统开发控制

ZJCA 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

ZJCA 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

ZJCA 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

ZJCA 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

ZJCA 暂不提供时间戳服务。

7. 证书、证书吊销列表和在线证书状态协议

7.1 证书

ZJCA 签发的证书均符合 X.509 V3 证书格式，遵循 RFC3280 标准。证书至少包含基本的 X.509v1 域，其规定值或值的限制如下表所描述。

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, ZJCA 签发的证书按照 RFC 3280 标准, 用 sha1RSA 算法签名
颁发者	颁发者的甄别名
证书有效期从	基于国际通用时间(UTC), 和北京时间同步, 按 RFC 3280 要求编码
证书有效期至	基于国际通用时间(UTC), 和北京时间同步, 按 RFC 3280 要求编码。有效期限的设置符合 ZJCA CP 6.3.2 规定的限制

证书有效期	基于国际通用时间(UTC)，和北京时间同步，按 RFC 3280 要求编码。有效期限的设置符合 ZJCA CP 6.3.2 规定的限制
主题	证书持有者或实体的甄别名
颁发者	为证书订户颁发该证书的认证机构
公钥	根据 RFC 3280 编码，使用 ZJCA CP 7.1.3 中指定的算法，密钥长度满足 ZJCA CP 6.1.5 指定的要求
签名	生成和编码满足 RFC 3280 的要求。

7.1.1 版本号

ZJCA 签发的证书符合 X.509 V3 标准。

7.1.2 证书扩展项

针对特别的用户，ZJCA 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

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参见本 CPS 6.1.7。

7.1.2.2 证书策略扩展项

证书策略扩展项中有 ZJCA 证书策略中对应证书类的 CP 对象标识符及策略限定符。

7.1.2.3 主体备用名

扩展项的使用符合 RFC 3280。

7.1.2.4 基本限制扩展项

ZJCA 证书的基本限制扩展项中的主体类型被设为 CA。最终订户证书的基本限制扩展项的主体类型设为最终实体。

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。对于最终订户证书签发 CA，其 CA 证书“Path Length Constraint”域的值设为“None”，表示证书路径中仅有一个最终订户证书可以跟在这个 CA 证书后面。

7.1.2.5 增强型密钥用法

对 ZJCA 不同的证书，扩展的密钥用法扩展项设定如下。

	CA 证书	个人证书		企业证书		设备证书	代码签名证书
		签名	加密	签名	加密		
客户端验证	set	set	Clear	set	Clear	set	set
安全电子邮件	set	set	Clear	set	Clear	set	set
加解密	set	Clear	set	Clear	set	set	set

7.1.2.6 CRL 的分发点

ZJCA 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

ZJCA 最终订户证书及中级 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 160 位的签发证书的 CA 的公钥进行 SHA-1 散列运算后的值构成；否则，它将包含签发 CA 的主体 DN 和序列号。

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。

7.1.3 算法对象标识符

ZJCA 签发的证书按照 RFC 3280 标准，用 sha1RSA 算法签名。

7.1.4 名称形式

ZJCA 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，O 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，O 代表证书签发机构，第一个 OU 签发机构中的部门或服务类（如 CN Individual Consumer Service Center）。甄别名可以包含不止一个的 OU 用于存放其他信息，如可将一个附加的组织部门(OU)域包含在最终订户证书中，该域指出证书对应的依赖方协议所在的 URL。

7.1.5 名称限制

参见本 CPS 3.1.2。

7.1.6 证书策略对象标识符

ZJCA 的每类证书对应一个证书策略对象标识符。当使用证书策略扩展项时，ZJCA 签发证书中包含证书策略对象标识符，该对象标识符与相应的证书类别对应。

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

与 ITU X.509 和 RFC3280 规定一致。

7.2 证书吊销列表

7.2.1 版本号

ZJCA 定期签发 CRL（证书废除列表），其所签发的 CRL 遵循 RFC3280 标准。采用 X.509 V2 格式。

7.2.2 CRL 和 CRL 条目扩展项

➤ 颁发者

CN = ZJCA

L = 杭州市

S = 浙江省

C = CN

➤ CRL 发布

ZJCA 每隔 24 小时自动发布最新的 CRL。

➤ 签名算法

ZJCA 采用 sha1 RSA 签名算法。

7.3 在线证书状态协议

ZJCA 为证书订户提供 OCSP 服务（在线证书状态查询服务），OCSP 为 CRL 的有效补充，方便证书订户及时查询证书状态信息。ZJCA OCSP 服务遵循 RFC2560 标准。OCSP 响应至少包含如下表所述基本域和内容。

域	值或值限制
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。使用 sha1 算法签名。
颁发者	签发 OCSP 的实体。颁发者公钥的 SHA1 数据摘要值和证书甄别名。
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(SHA1)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

8.1 评估的频率或情形

审计是为了检查和监督 ZJCA 及其下属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》、《ZJCA 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 ZJCA 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、保障客户权益的目的。

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 ZJCA 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。

外部审计原则上每年执行一次。

内部审计是指 ZJCA 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 ZJCA 内部用以完善管理、改进服务，不需对外公开。

内部审计按 ZJCA 自身需求确定其频率。

8.2 评估者的资质

对 ZJCA 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。

8.3 评估者与被评估者之间的关系

评估者应是与被评估者无任何业务、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

ZJCA 管理层将对审计报告进行评估，对于在审计中发现的重大以外或不作为采取行动。根据审计中发现的意外或不作为对证书体系的安全或完整性的危险程度制定相应的改动计划，必须在 30 天内制定改正行动计划，并在合理的期限内执行它。

8.6 评估结果的传达与发布

除非法律明确要求，ZJCA 一般不公开审计结果。

在必要的情况下，向 ZJCA 关联单位（例如垫付商、注册机构、审核受理点）通知审计结果的具体规定将在 ZJCA 和关联单位的协议中写明。

9. 法律责任和其他业务条款

9.1 费用

9.1.1 证书签发和更新费用

ZJCA 对证书签发收费及标准参照“浙价服[2006]154号”文件。

ZJCA 对证书更新暂时不收取费用，但保留对该服务收费的权利。

9.1.2 证书查询费用

ZJCA 对证书查询暂时不收取费用，但保留对该服务收费的权利。

9.1.3 证书吊销或状态信息的查询费用

ZJCA 对证书吊销或状态信息的查询暂时不收取费用，但保留对该服务收费的权利。

9.1.4 其他服务费用

根据 ZJCA 向订户提供的认证服务内容，如证书恢复、密钥托管以及其它一些服务所需要的工本费，其具体标准在网站及时公布。

9.1.5 退款策略

如果由于 ZJCA 的原因，造成订户合同无法履行、订户证书无法使用，ZJCA 会将有关费用返还给订户。

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

9.2 财务责任

9.2.1 保险范围

ZJCA 根据业务发展情况和国内保险公司的业务开展情况决定其投保策略。

9.2.2 其他资产

无规定。

9.2.3 对最终实体的保险或担保

根据《中华人民共和国电子签名法》的规定，订户在此同意：由于 ZJCA 的责任给订户造成的直接损失，ZJCA 将根据使用证书的种类，承诺赔偿订户一定金额的直接损失。具体的情况及赔付额度，参见本 CPS 9.9。

9.3 业务信息的保密

9.3.1 保密信息范围

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。

客户信息：客户的注册信息；客户系统、应用访问 CRL、OCSP 的记录（时间、频度）；客户与认证机构、注册机构签订的协议；

9.3.2 不属于保密的信息

证书策略、认证业务声明、依赖方协议、订户协议等。

9.3.3 保护保密信息责任

ZJCA 通过有效的技术手段和管理程序，保护商业的和客户的保密信息。ZJCA 的每个员工都要接收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

隐私保密计划遵守现行的法律和法规。

9.4.2 作为隐私处理的信息

作为隐私处理的信息包括，最终订户注册申请证书中提交的信息，包括联系电话、地址等；个人与认证机构、注册机构签订的协议。

9.4.3 不被视为隐私的信息

出现在证书中的信息；证书及证书状态。

9.4.4 保护隐私的责任

认证机构、注册机构在没有获得客户授权的情况下，不得将客户隐私信息透露给第三方。但在法律法规或公共权力部门通过合法程序要求下，ZJCA 可以向特定的对象公布隐私信息，ZJCA 无需承担由此造成的任何责任。

9.4.5 使用隐私信息的告知与同意

认证机构、注册机构如果需要将客户隐私信息用于业务范围内，无论是否涉及到隐私，ZJCA 均可以不用告知订户；但在用于双方约定的用途以外的目的，则需要事先告知客户并获得客户同意和授权，而且这种同意和授权是要用可归档的方式（如传真、信函、电子邮件等）。

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，认证机构、注册机构将有关信息在客户知晓或不知晓的情况下提供有关执法机关、行政执行机关是允许的，即使这样，认证机构、注册机构也应尽可能地保护客户隐私信息。

9.4.7 其他信息披露情形

ZJCA、订户、注册机构、依赖方等机构或个人都有义务按照本 CPS 的规定，承担相应的保护隐私责任。ZJCA、订户、注册机构、依赖方等机构或个人对其他信息的披露受制于法律、订户协议。

9.5 知识产权

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

按本 CPS 的规定，所有与 ZJCA 发行的证书和 ZJCA 提供的软件相关的一切版权、商标和其他知识产权均属于 ZJCA 的产权，这些知识产权包括所有相关的文件和使用手册。电子认证服务机构在征得 ZJCA 的同意后，可以使用相关的文件和手册，并有责任和义务提出修改意见。

在没有 ZJCA 预先书面同意的情况下，任何使用者不能在任何证书到期、作废或终止后，使用或接受任何 ZJCA 使用的名称、商标、交易形式或可能与之相混淆的名称、商标、交易形式或商务称号。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

订户同意订户协议是作为订户注册申请的一个条件，依赖方同意依赖方协议作为接收证书及状态信息的一个条件。同样地，认证机构必须按要求使用订户协议和依赖方协议。电子认证服务机构不负责评估证书是否被恰当使用。订户和依赖方必须依订户协议和依赖方协议确保证书用于允许使的目的。认证机构和订户之间的担保、免责和有限责任由他们之间的协议规定和约束。

认证机构对证书订户必须做出如下担保：

证书中不存在批准证书申请或签发证书的实体已知的对事实的实质性错误描述，或来自于这些实体的错误信息。

在管理证书申请或制造证书时，批准证书申请或签发证书的实体不会因为工作疏忽将错误信息包含到了证书中。

他们的证书满足本 CPS 所有实质性的要求。

吊销服务和信息库的使用在所有方面符合本 CPS 的要求。

认证机构对证书依赖方必须做出如下担保：

除了未经鉴证的订户信息外，包含在证书中的所有信息都是准确的。

在认证机构信息库中发布的证书已经签发给个人或组织机构（它们的名字包含在证书中），订户已经根据接收了该证书。

批准证书申请或签发证书的实体签发证书时完全遵守了本 CPS 的规定。

除此之外，认证机构还可以提供其他的担保。

9.6.2 注册机构的陈述与担保

注册机构必须做出如下担保：

注册机构在批准证书前，完成了所有必要的确认工作，并且需确认的信息是正确的、准确的。

9.6.3 订户的陈述与担保

作为获得证书的一个条件，证书申请人在证书申请时已阅读了订户协议并且同

意订户协议，并且：利用与证书中的公钥相对应的私钥产生的电子签名是订户的数字签名，订户知晓要签名的内容，产生电子签名时，订户已经接收了证书，且该证书没有过期或吊销。

保护自己的私钥，没有经过授权的人员不得访问订户的私钥。

在证书申请时，订户的所有陈述都是对的。

订户提供的和包含在证书中的所有信息都是对的。

证书只能按照本 CPS 用于经过授权的或其它合法的使用目的。

不将证书用于与证书使用目的以外的场合。

9.6.4 依赖方的陈述与担保

在任何依赖行为发生之前，依赖方阅读必须依赖方协议，独立评估证书使用于任何目的适当性，并确定证书将会被恰当地使用于本 CPS 所规定的目的。

9.6.5 其他参与者的陈述与担保

无规定。

9.7 担保免责

ZJCA 不对由于客观意外或其他不可抗力事件造成的操作失败或延迟承担任何损失、损坏或赔偿责任。这些事件包括劳动纠纷、交易一方故意或无意的行为、罢工、暴动、骚动、战争、火灾、爆炸、地震、水灾或其他大灾难等。

ZJCA 在提供给证书持有者的“电子签名认证证书申请责任书”中，都有事先告知证书持有者的免责条款的规定：ZJCA 发放的各类型证书只能用于网络上标识身份、加密数据、保证网络安全通讯等相应证书规定的用途，不能作为其他任何用途。若证书持有者将其证书用于其他的用途，ZJCA 不承担任何责任。ZJCA 在进行申请者身份认证或证书制作时，将充分遵守 ZJCA 的安全操作流程。如果由于非 ZJCA 的原因而造成的 ZJCA 设备故障、线路中断，导致签发证书错误、延误、中断或者无法签发，ZJCA 不负任何赔偿责任。

ZJCA 在签发证书之前，证书申请者已同意遵守“电子签名认证证书申请责任书”中的各项规定。责任书中明确规定 ZJCA 不承担任何形式的担保和义务。如果证书申请者故意或无意地提供不完整、不可靠或已过期的信息，而又根据正常的流程提供了必须的审核文件，由此得到了 ZJCA 签发的证书，由此引起的法律和经济责任由证书申请者全部承担，ZJCA 不承担与证书内容相关的法律和经济责任，但可以根

据受害者的请求提供协查帮助。ZJCA 也不承担任何其他未经授权的人或组织以 ZJCA 名义编撰、发表或散布不可信赖的信息所引起的法律责任。ZJCA 仅仅提供电子沟通或交易中签名的“不可抵赖”的依据，但并不表明有对此承担法律责任等方面的约定。

9.8 有限责任

在法律允许的范围内，认证机构订户协议、依赖方协议和其他订户协议限制认证机构承担的责任。责任限制包括排除间接的、特殊意外造成的、偶然的和后续性的损失。

9.9 赔偿

ZJCA 及其授权的发证机构，对所有当事人（包括但不限于订户、申请者、接受者或依赖方）的合计赔偿额度，其最高限度不超过如下金额：

1. 个人证书每张最高为 3600 元；
2. 单位证书每张最高为 10000 元；
3. 设备证书每张最高为 40000 元。

在如下情况，认证机构对自身原因造成的订户损失对订户进行赔偿，或依赖方在履行了依赖方协议的情况下，由于认证机构或订户的原因造成的依赖方损失，认证机构对依赖方的赔偿。认证机构可通过购买第三方保险对赔偿进行覆盖。

认证机构在批准证书前没有执行程序确认证书申请，造成证书的错误签发；

由于认证机构的原因，使得证书中出现了错误信息；

由于认证机构 CA 私钥的泄漏。

在如下情况，订户对自身原因造成的认证机构、依赖方损失对认证机构进行赔偿。订户可通过购买第三方保险对赔偿进行覆盖。

订户在证书申请中对事实的虚假或错误时描述；

在证书申请中订户没有披露重要的事实，如果这种错误表述或遗漏是因为粗心或故意欺骗任何一方；

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；

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法。

在如下情况，依赖方对自身原因造成的认证机构损失对认证机构进行赔偿。依赖方可通过购买第三方保险对赔偿进行覆盖。

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。

9.10 有效期限与终止

9.10.1 有效期限

作为认证机构的核心业务文件，CPS 和 CP 在认证机构终止业务前一直有效，在发布新的 CPS 和 CP 版本后，新的 CPS 和 CP 版本将取代原 CPS 和 CP 版本。对于证书订户而言，证书签发时的 CPS 和 CP 和订户协议将起作用直到证书到期或吊销，除非法律相冲突的内容、与事实不符的错误描述。对某一特定证书而言，在公钥的有效使用期限内，依赖方协议有效。公钥的有效使用期限可以比证书有效期长，比如签名证书到期后，公钥可以继续对证书有效期内私钥签名的信息进行验证。其他合同、协议的有效期限，由相应的合同、协议约定。

9.10.2 终止

当认证机构中止业务时，CPS 和 CP 即终止。当证书到期或吊销后，订户协议即终止。公钥到了的有效使用期，对应的依赖方协议终止。

9.10.3 效力的终止与保留

CPS 和 CP 的中止，而非更新，意味着认证机构认证业务的终止，但认证业务的终止不意味着认证机构责任的终止。认证机构在业务终止后应采取合理的措施，保证订户的利益，如证书可继续使用，对客户进行赔偿，或将认证服务转到其他认证机构。订户证书到期、证书吊销意味着订户协议的终止，认证机构不再对证书私钥（签名）或公钥（加密）的使用承担任何责任，依赖方不应再信赖证书对应的签名私钥或加密公钥。

当由于某种原因，如内容修改、与适用法律相冲突，CPS、CP、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 对参与者的个别通告与沟通

认证机构在必要的情况下，如主动吊销订户证书、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，可通过适当方式，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

ZJCA 安全认证管理委员会每年至少审查一次本 CPS，确保其符合国家法律法规和主管部门的要求，符合认证业务开展的实际需要。

本 CPS 的修订由 ZJCA 办公室提出并修改，ZJCA 安全认证管理委员会审核并批准后才能予以发布。

9.12.2 通知机制与期限

修改后的 CPS 经批准后将立即在 ZJCA 信息库更新通告栏发布。对于需要通过电子邮件、信件等方式通知的修改，ZJCA 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

当本 CPS 描述的规则、流程和相关技术已经不能满足 ZJCA 电子认证业务要求或本 CPS 依据的法律法规和部门规章变更时，ZJCA 将依照有关规定修改本 CPS 的相关内容。

9.13 争议处理

如果当事人之间无法很好的解决出现的问题和争端，应该提交仲裁机构，根据仲裁条例在时效内裁决。仲裁的决定是终决性的，对每个当事人都有约束力。

9.14 管辖法律

中华人民共和国法律、规则、规章、法令和政令将管辖认证机构的业务活动。认证机构的任何业务活动必须受有关法律、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

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

ZJCA 提供的电子认证服务遵循《电子认证服务密码管理办法》。

9.16 一般条款

9.16.1 完整协议

CPS、CP、订户协议及依赖方协议及其补充协议将构成 PKI 参与者之间的完整协议。

9.16.2 转让

认证机构、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

在法律允许的范围内，认证机构的订户协议、依赖方协议和其他订户协议可以包含可分割性条款。一个协议中的可分割性条款防止协议中一个条款的无效影响协议中其他条款效力。

9.16.4 强制执行

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

9.16.5 不可抗力

在法律允许的范围内，认证机构的订户协议、依赖方协议和其他订户协议应该包括保护不可抗力条款，明确在出些哪些不可抗拒力情况下，认证机构可以免除或部分免除责任。一般地，自然灾害、战争属于不可抗拒力。

9.17 其他条款

无规定。