



JSCA CPS

JSCA 认证业务声明

版本 1.3.0

生效日期：2011 年 4 月 1 日

JSCA CPS

Certification Practice Statement

Version 1.3.0

Effective Date: Apr. 1st 2011

保密事宜:

本文档包含江苏省电子商务证书认证中心有限公司（以下简称 JSCA）的专有商业信息和保密信息。

接受方应当维护本文档全部信息的保密性，承诺不进行复制，或向除评估小组以外的其他非直接相关的人员公开此信息。对于以下三种信息，接受方可以免除承担保密责任：

- 1) 接受方在接收该文档前，已经掌握的信息。
- 2) 可以通过公开渠道获得的信息。
- 3) 可以从第三方，以无附加保密要求方式获得的信息。

目 录

1	概括性描述	1
1.1	概述	1
1.2	文档名称与标识	2
1.3	电子认证活动参与者	2
1.3.1	电子认证服务机构	3
1.3.2	注册机构	4
1.3.3	用户	4
1.3.4	依赖方	5
1.3.5	其它参与者	5
1.4	证书应用	5
1.4.1	适合的证书应用	5
1.4.2	限制的证书应用	6
1.5	策略管理	6
1.5.1	策略文档管理机构	6
1.5.2	联系人	6
1.5.3	决定 CPS 符合策略的机构	6
1.5.4	CPS 批准程序	6
1.5.5	定义和缩写	7
2	信息发布与信息管理	9
2.1	信息库	9
2.2	认证信息的发布	10
2.3	发布的时间或频率	10
2.4	信息库访问控制	10
3	身份识别与鉴别	10
3.1	命名	10
3.1.1	名称类型	10
3.1.2	对名称意义化的要求	10

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话: 025-83393092 传真: 025-83393091

URL: <http://www.jsca.com.cn>

3.1.3	理解不同名称形式的规则	11
3.1.4	名称的惟一性	12
3.2	初始身份确认	12
3.2.1	证明拥有私钥的方法	12
3.2.2	组织机构身份的鉴别	13
3.2.3	个人身份的鉴别	13
3.2.4	没有验证的用户信息	13
3.2.5	互操作准则	14
3.3	密钥更新请求的标识与鉴别	14
3.3.1	常规密钥更新的标识与鉴别	14
3.3.2	吊销后密钥更新的标识与鉴别	14
3.3.3	吊销请求的标识与鉴别	14
4	证书生命周期操作要求	15
4.1	证书申请	15
4.1.1	证书申请实体	15
4.1.2	注册过程与责任	15
4.2	证书申请处理	15
4.2.1	执行识别与鉴别功能	15
4.2.2	证书申请批准和拒绝	16
4.2.3	处理证书申请的时间	16
4.3	证书签发	16
4.3.1	证书签发中注册机构和电子认证服务机构的行为	16
4.3.2	电子认证服务机构和注册机构对用户的通告	16
4.4	证书接受	17
4.4.1	构成接受证书的行为	17
4.4.2	电子认证服务机构对证书的发布	17
4.4.3	电子认证服务机构对其他实体的通告	17
4.5	密钥对和证书的使用	17

4.5.1	用户私钥和证书的使用	17
4.5.2	依赖方公钥和证书的使用	17
4.6	证书更新	18
4.6.1	证书更新的情形	18
4.6.2	请求证书更新的实体	18
4.6.3	证书更新请求的处理	18
4.6.4	颁发新证书时对用户的通告	18
4.6.5	构成接受更新证书的行为	19
4.6.6	电子认证服务机构对更新证书的发布	19
4.6.7	电子认证服务机构对其他实体的通告	19
4.7	证书密钥更新	19
4.7.1	证书密钥更新的情形	19
4.7.2	请求证书密钥更新的实体	20
4.7.3	证书密钥更新请求的处理	20
4.7.4	颁发新证书时对用户的通告	20
4.7.5	构成接受密钥更新证书的行为	20
4.7.6	电子认证服务机构对密钥更新证书的发布	20
4.7.7	电子认证服务机构对其他实体的通告	20
4.8	证书变更	21
4.8.1	证书变更的情形	21
4.8.2	请求证书变更的实体	21
4.8.3	证书变更请求的处理	21
4.8.4	颁发新证书时对用户的通告	21
4.8.5	构成接受变更证书的行为	21
4.8.6	电子认证服务机构对变更证书的发布	22
4.8.7	电子认证服务机构对其他实体的通告	22
4.9	证书吊销和挂起	22
4.9.1	证书吊销的情形	22

4.9.2	请求证书吊销的实体	23
4.9.3	吊销请求的流程	23
4.9.4	吊销请求宽限期	23
4.9.5	电子认证服务机构处理吊销请求的时限.....	23
4.9.6	依赖方检查证书吊销的要求	23
4.9.7	CRL 发布频率	23
4.9.8	CRL 发布的最大滞后时间.....	24
4.9.9	在线的吊销/状态查询的可用性.....	24
4.9.10	在线的吊销查询要求	24
4.9.11	吊销信息的其他发布形式	24
4.9.12	对密钥遭攻击的特别处理要求.....	24
4.9.13	证书挂起的情形.....	24
4.9.14	请求证书挂起的实体	25
4.9.15	挂起请求的流程.....	25
4.9.16	挂起的期限限制.....	25
4.10	证书状态服务	25
4.10.1	操作特征.....	25
4.10.2	服务可用性	26
4.10.3	可选特征.....	26
4.11	订购结束.....	26
4.12	密钥生成、备份与恢复.....	26
4.12.1	密钥生成、备份与恢复的策略与行为.....	26
4.12.2	会话密钥封装和恢复策略与行为	26
5	认证机构设施、管理和操作控制	26
5.1	场地位置与建筑.....	26
5.1.1	物理访问	27
5.1.2	电力与空调.....	28
5.1.3	水患防治	28

5.1.4	火灾防护	28
5.1.5	介质存储	28
5.1.6	废物处理	29
5.1.7	异地备份	29
5.2	程序控制	29
5.2.1	可信角色	29
5.2.2	每项任务需要的人数	29
5.2.3	每个角色的识别与鉴别	30
5.2.4	需要职责分割的角色	30
5.3	人员控制	30
5.3.1	资格、经历和无过失要求	30
5.3.2	背景审查程序	30
5.3.3	培训要求	31
5.3.4	再培训周期和要求	31
5.3.5	工作岗位轮换周期和顺序	31
5.3.6	未授权行为的处罚	31
5.3.7	独立合约人的要求	32
5.3.8	提供给员工的文档	32
5.3.9	关键岗位人员离职	32
5.4	审计日志程序	32
5.4.1	记录事件的类型	32
5.4.2	处理日志的周期	34
5.4.3	审计日志的保存期限	34
5.4.4	审计日志的保护	34
5.4.5	审计日志备份程序	34
5.4.6	审计收集系统	34
5.4.7	对导致事件实体的通告	34
5.4.8	脆弱性评估	35

5.5	记录归档.....	35
5.5.1	归档记录的类型	35
5.5.2	归档记录的保存期限	35
5.5.3	归档文件的保存方式	35
5.5.4	归档文件的备份程序	35
5.5.5	记录时间戳要求.....	36
5.5.6	归档收集系统	36
5.5.7	获得和检验归档信息的程序	36
5.6	电子认证服务机构密钥更替	36
5.7	损害与灾难恢复.....	36
5.7.1	事故和损害处理程序	37
5.7.2	计算资源、软件和数据损坏	37
5.7.3	实体私钥损害处理程序	38
5.7.4	灾难后的业务连续性能力	38
5.8	电子认证服务机构或注册机构的终止	38
6	认证系统技术安全控制	39
6.1	密钥对的生成和安装	39
6.1.1	密钥对的生成	39
6.1.2	私钥传送给用户	39
6.1.3	公钥传送给证书签发机构.....	39
6.1.4	电子认证服务机构公钥传送给依赖方	40
6.1.5	密钥的长度.....	40
6.1.6	公钥参数的生成和质量检查	40
6.1.7	密钥使用目的	40
6.2	私钥保护和密码模块工程控制.....	40
6.2.1	密码模块的标准和控制	40
6.2.2	私钥多人控制 (m 选 n)	41
6.2.3	私钥托管	41

6.2.4	私钥备份	41
6.2.5	私钥归档	41
6.2.6	私钥导入、导出密码模块.....	42
6.2.7	私钥在密码模块的存储	42
6.2.8	激活私钥的方法	42
6.2.9	解除私钥激活状态的方法.....	42
6.2.10	销毁私钥的方法.....	42
6.2.11	密码模块的评估.....	43
6.3	密钥对管理的其他方面.....	43
6.3.1	公钥归档	43
6.3.2	证书操作期和密钥对使用期限	44
6.4	激活数据.....	44
6.4.1	激活数据的产生和安装	44
6.4.2	激活数据的保护	44
6.4.3	激活数据的其他方面	44
6.5	计算机安全控制.....	45
6.5.1	特别的计算机安全技术要求	45
6.5.2	计算机安全评估	45
6.6	网络的安全控制.....	45
6.7	时间戳.....	46
7	证书、证书吊销列表和在线证书状态协议.....	46
7.1	证书	46
7.1.1	版本号	46
7.1.2	算法对象标识符	46
7.1.3	名称形式	46
7.1.4	名称限制	48
7.1.5	证书策略对象标识符	49
7.1.6	策略限制扩展项的用法	50

7.1.7	策略限制符的语法和语义.....	50
7.1.8	关键证书策略扩展项的处理规则.....	50
7.2	CRL	50
7.2.1	版本号	50
7.2.2	CRL 和 CRL 条目扩展项	50
7.3	在线证书状态协议	51
8	认证机构审计与评估.....	52
8.1	审计内容.....	52
8.2	审计的频率与条件	52
8.2.1	JSCA 的审计	52
8.2.2	JSCA 对关联单位的审计	52
8.3	审计者的身份与资质	53
8.3.1	JSCA 的内部审计	53
8.4	不足信息的处理.....	53
8.5	审计结果.....	53
9	法律责任和其他业务条款	54
9.1	费用	54
9.1.1	费用支付	54
9.1.2	证书费用	54
9.2	财务责任.....	54
9.3	业务信息保密	54
9.3.1	保密信息范围	55
9.3.2	不属于保密的信息.....	55
9.3.3	保护机密信息的责任	56
9.4	个人隐私保密	56
9.4.1	隐私保密方案	56
9.4.2	作为隐私处理的信息	56
9.4.3	不被视作隐私的信息	56

9.4.4	保护隐私的责任	57
9.4.5	使用隐私信息的告知与同意	57
9.4.6	依法律或行政程序的信息披露	57
9.4.7	其他信息披露情形	57
9.5	知识产权	57
9.6	陈述与担保	58
9.6.1	电子认证服务机构的陈述与担保	58
9.6.2	注册机构的陈述与担保	59
9.6.3	用户的陈述与担保	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	理赔	61
9.9.1	JSCA 承担责任的限制	61
9.9.2	注册机构承担责任的限制	61
9.9.3	注册分支机构责任的限制	62
9.9.4	受理点承担责任的限制	62
9.10	有效期限和终止	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	63
9.12	修订	63
9.12.1	修订程序	63
9.12.2	通知机制和期限	63
9.12.3	必须修改业务规则的情形	64
9.13	争议处理	64

9.14	管辖法律.....	64
9.15	适用的法律的符合性.....	64
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.....	65
9.16.4	强制执行.....	65
9.16.5	不可抗力.....	65
9.17	其它条款.....	65
9.17.1	各种规范的冲突.....	65
9.17.2	安全资料的财产权益.....	65

1 概括性描述

1.1 概述

电子认证业务规则（CPS, Certification Practice Statement）是关于认证机构（CA, Certification Authority）在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）所必须遵循的规范并详细的描述和声明，同时提供涉及业务、技术和法律方面的细节。JSCA 根据 ISO 组织 IETF RFC 3647 规范编写了本单位 CPS，作为 JSCA 证书相关业务和系统运行的规范。

本文档的编写遵从 IETF RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, 公钥基础设施证书策略和证书运行框架)、十届全国人大常委会表决通过的并于 2005 年 4 月 1 日正式实施的《中华人民共和国电子签名法》以及中华人民共和国工业和信息化部修订并通过的《电子认证服务管理办法》。

JSCA 是指江苏省电子商务证书认证中心有限责任公司 (Jiangsu Certification Authority Co., Ltd)，是经国家工业和信息化部、国家密码管理局批准成立的，全国性、公正可信的第三方认证机构。公司由江苏省国信资产管理集团有限公司等多家省内大型机构联合组建，应用目前领先的密码加密技术，为电子政务外网和电子商务网络提供数字证书安全认证服务。

JSCA 自成立以来，严格按照国家规定的各项要求运作。2004 年 4 月，江苏省数字证书认证中心建设实施方案通过了国家密码管理委员会办公室组织的专家论证。2004 年 12 月 6 日，JSCA 通过了国家密码管理委员会办公室组织的安全性审查。2005 年 9 月 6 日，JSCA 通过了国家密码管理局组织的技术鉴定，于 2005 年 12 月 26 日获得国家工业和信息化部颁发的《电子认证服务许可证》。2010 年 11 月，JSCA 获得国家密码管理局许可授权为政府部门开展社会管理和公共服务等政务活动提供电子认证服务。

JSCA 为互联网的交易多方建立信任关系以保证交易主体身份的真实性，为

信息的保密性、完整性以及交易的不可抵赖性提供全面服务。作为被信任的第三方, JSCA 或 JSCA 授权的发证机构为网上交易和网上安全操作的参与人颁发数字证书。JSCA 数字证书(以下简称证书)遵循 X. 509V3 规范。JSCA 承诺, 在证书有效的情况下, 保证证书能唯一地与身份明确的实体相关联, 公钥能与身份确定的实体唯一相对应。

为配合证书业务的正常开展, JSCA 编写了 JSCA 认证业务声明。认证业务声明的建立及其正确的贯彻和实施将为江苏省电子政务公共服务、电子交易和其他网上安全服务提供强有力的支持。

JSCA 提供证书与信息安全服务的商用 PKI 系统主要特点为:

- 1) 提供完善的 PKI 系统的核心服务和扩展服务;
 - 核心服务包括: 认证服务、加密服务、完整性服务;
 - 扩展服务包括: 安全通讯服务、公证服务、不可否认服务、时间戳服务、其它扩展服务;
- 2) 遵循国际开放标准(包括 PKCS 系列、PKIX 系列、X.500 和 X.509 系列等), 且随着标准化进程持续促进技术的不断发展;
- 3) 支持多证书、多密钥对、多算法, 支持解密密钥托管;
- 4) 具有对证书生命期的全程自动管理并且对用户透明;
- 5) 体系结构扩展性好, 支持和其它 CA 互联互通。

1.2 文档名称与标识

本文为 JSCA 电子认证业务规则(CPS), 并在 JSCA 网站发布。JSCA 网址:
<http://www.jsca.com.cn>。

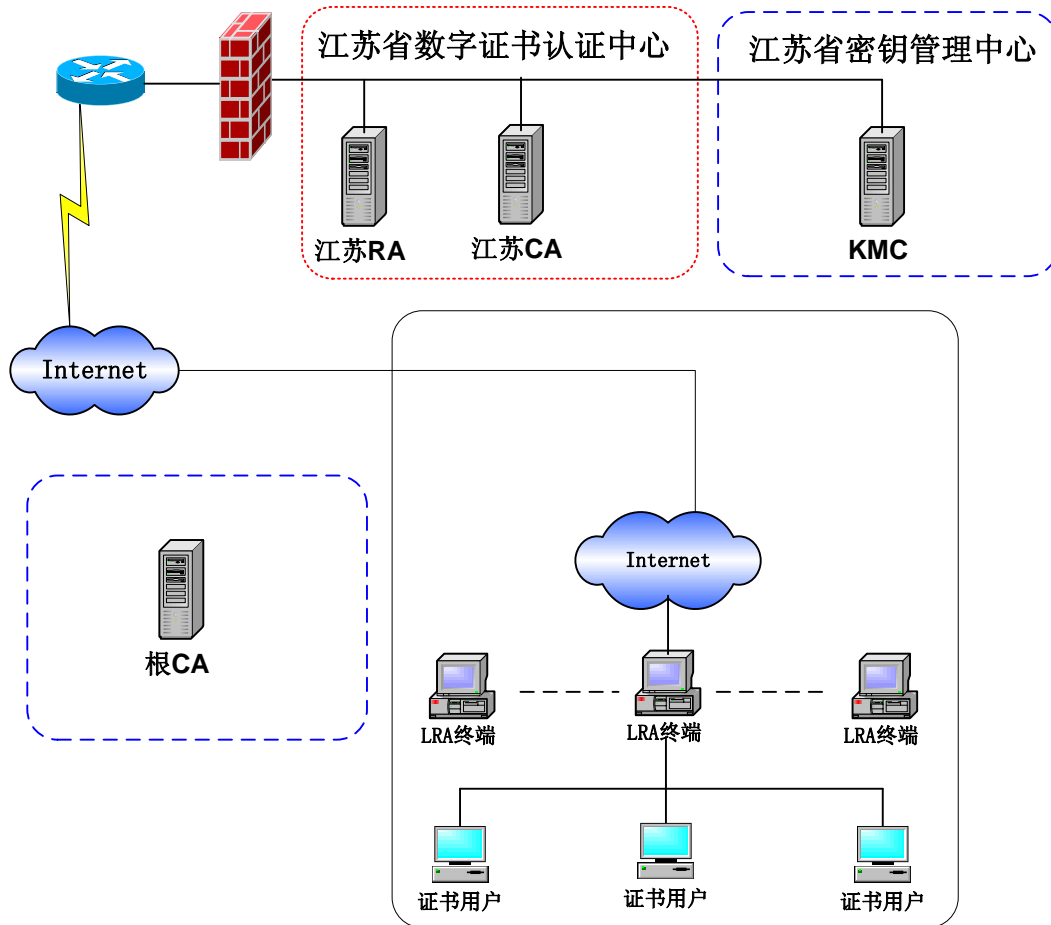
1.3 电子认证活动参与者

JSCA 认证系统采用国际领先的 PKI 技术, 总体为两层 CA 结构, 第一层为根 CA; 第二层为运营 CA, 根据电子认证业务规则(CPS)发放证书。以下为 JSCA 认证系统结构图示:

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话: 025-83393092 传真: 025-83393091

URL: <http://www.jsca.com.cn>



1.3.1 电子认证服务机构

JSCA 和 JSCA 下层 CA 统称为电子认证服务机构。

JSCA 是所有 JSCA 下层机构和实体的根。在十分严密的保密和安全机制控制下，JSCA 根据根证书有效的安全策略自己生成密钥对，自己签发根证书。JSCA 根据授权和协议，签发下一级证书。JSCA 将决定在什么时间、什么地点、由什么人监督、怎么实施 JSCA 根密钥对的更新和切换。JSCA 的动作单位是江苏省电子商务证书认证中心有限责任公司。JSCA 已经建立了完善的安全机制，以保证私有密钥的安全性。在时机成熟的时候，JSCA 还将建立异地备份中心。

JSCA 所签发的证书与每一个证书申领实体的公钥绑定。JSCA 承诺，在有效期内的证书，将采用证书目录服务器和证书黑名单服务器 CRL SERVER，公布该

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

证书可以公开的信息和状态。

1.3.2 注册机构

注册机构 RA(Registration authority)系统负责用户证书的申请、审批和证书管理，直接面向证书用户，并将证书申请信息传递到 CA。

JSCA 的 RA 系统分为本地 RA 和自建 RA。

本地 RA 指 RA 服务器设立在 JSCA 的 RA 系统，归 JSCA 所有，由 JSCA 使用，适合于不建立 RA 系统、没有 RA 操作人员的机构和组织使用。

自建 RA 指 RA 服务器设立在机构或组织中的 RA 系统，归机构或组织所有，由机构或组织使用，为证书总量较大或证书审核严格或证书管理复杂的机构或组织提供证书申请审批、证书信息录入以及证书发放并进行部分管理服务，采用安全方式与 JSCA 连接。RA 服务器通过 Internet 或者专线按照 CA 的接口与 JSCA 系统直接相连，进行数据和指令的传输。

RA 系统一般为两层结构，分为 RA 服务器和 RA 受理点 LRA。LRA 是面向最终用户的注册审核机构，其主要功能是对用户提交的资料进行审核，以决定是否同意为该申请者发放证书。LRA 的身份由 RA 审核，LRA 的操作员证书由运行 CA 签发。LRA 作为 RA 的下级机构，它不直接与 CA 进行数据交换，CA 不接收来自 LRA 的证书签发请求，LRA 的证书签发请求由 RA 转发给 CA。RA 服务器负责安全地和 JSCA 的 CA 服务器交换数据。

1.3.3 用户

“用户”是指从电子认证服务机构接受证书的实体。在电子签名应用中，“用户”即为电子签名人。“用户”也可称为证书和证书相关服务的使用者。在本 CPS 中，“订户”与“用户”具备同等含义。

目前 JSCA 的数字证书在电子商务和面对公众服务的电子政务外网有广泛的应用用户群体。

1.3.4 依赖方

依赖方是依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个用户。在 JSCA 体系中，是信任 JSCA 证书，可以对使用 JSCA 证书机制进行的数字签名进行验证，使用其他 JSCA 证书用户的公钥加密信息的实体。

1.3.5 其它参与者

其他参与者包括：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。在 JSCA 证书应用系统中除了 JSCA、依赖方、终端用户以外的参与方统一称为其它参与者。

1.4 证书应用

1.4.1 适合的证书应用

JSCA 通过发放数字证书为电子商务和电子政务活动提供安全保障：确保互联网上信息传递双方身份的真实性、信息的保密性、完整性以及网上交易的不可否认性。JSCA 证书只能用于证书策略规定的合法目的。按照证书的功能及使用证书的实体的不同，JSCA 提供包括且不限于以下所列的多种证书：

机构证书——提供 Web 服务器、浏览器以及应用系统之间提供证书验证、信息加密、数字签名和目录服务等功能。适用于机构网上交易，安全级别高，功能强劲。

个人证书——与国内绝大多数建立在 SSL 协议上的证书应用类似，适用于个人网上身份认证和电子商务交易。

服务器证书——用于 Web Server 端的验证、数字签名以及建立安全会话通道等，保护服务器的信息安全。

安全电子邮件证书——用于安全收发电子邮件以及双方身份认证的证书。

VPN 证书----用于虚拟专用网的证书，解决了远程接入、分支机构和广域网的连接等对身份认证、信息完整性、私密性的安全应用需求。

1.4.2 限制的证书应用

对于使用未经 JSCA 认可的证书安全应用系统，不适用 JSCA 证书；

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

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 的制订、更新、发布等事宜，其管理机构为 JSCA CPS 编写和管理组。

1.5.2 联系人

马圣东----电话：025-83391997 email: masd@jsca.com.cn

1.5.3 决定 CPS 符合策略的机构

曹 晖----电话：025-83393098 email: ch@jsca.com.cn

1.5.4 CPS 批准程序

JSCACPS 批准流程是：

- 1) 发现 CPS 中所列条款不能适应运营的实际需求,或者与现行法律相抵触;
- 2) 将现存问题反馈 CPS 编写小组;
- 3) 经过 CPS 编写小组讨论后,提出具体的修改意见;
- 4) 修改意见提交安全管理小组;

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

- 5) 安全管理小组审查修改意见，如果不通过则提出修改意见书反馈给 CPS 编写小组；
- 6) CPS 修改意见经安全管理小组审查通过，由 CPS 编写小组发布更新。

1.5.5 定义和缩写

PKI 公钥基础设施 (Public Key Infrastructure)

是利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，使得互联网环境的身份鉴别、信息加解密、数据完整性和不可否认性服务得以实现。

CA 认证中心 (Certification Authority)

受用户信任的，负责创建和签发数字证书的权威机构。CA 是认证中心的英文 Certification Authority 的缩写。CA 中心，又称为数字证书认证中心。CA 中心作为电子交易中受信任的第三方，负责为电子商务环境中各个实体颁发数字证书，以证明各实体身份的真实性，并负责在交易中检验和管理证书。

RA 注册机构 (Registration authority)

负责用户证书的申请、审批和证书管理部分工作，面向证书用户。可以分为本地 RA 和自建 RA 两种。

本地 RA

指 RA 服务器设立在 JSCA 的 RA 系统。

自建 RA

指 RA 服务器设立在机构或组织中的 RA 系统，归机构或组织所有，由机构或组织使用，为证书审核严格或证书管理复杂的机构或组织提供证书申请审批、证书信息录入以及证书发放并进行部分管理服务的 RA 系统。

数字证书 (Digital Certificate)

数字证书又称为电子证书，是指经 CA 数字签名的包含证书使用者身份公开信息和公开密钥的电子文件。

由于 Internet 中电子商务系统技术使某些敏感或有价值的数字数据有被滥用的风险，为了保证互联网上电子交易及支付的安全性、保密性等，防范交易及支付过程中的欺诈行为，必须在网上建立一种信任机制。这就要求参加电子商务的各方都必须拥有合法的身份，并且在网上能够有效无误的被进行验证。数字证书提供了一种在 Internet 上验证身份的方式，其作用类似于日常生活中的身份证或护照以及驾驶证。

在本标准中，术语“数字证书”与“电子证书”可互换使用。

CRL 证书吊销列表 (Certificate Revocation List)

证书吊销列表(Certificate Revocation List, 简称 CRL), 是一种包含注销的证书列表的签名数据结构。CRL 是证书注销状态的公布形式, CRL 就像信用卡的黑名单, 它通知其他证书用户及依赖方某些数字证书不再有效。

LDAP (Lightweight Directory Access Protocol)

即轻量级目录访问协议, 用于查询、下载数字证书以及数字证书废止列表 (CRL)。

OCSP 在线证书状态协议 (Online Certificate Status Protocol)

暂未提供服务。

DTS (Digital Time Stamp)

即数字时间戳服务, 向用户提供可信的精确时间源, 以证明某个特定时间某个交易或者文档确实存在。

JSCA 时间服务器采用的是国际标准时间 UTC, 通过拨号接收国家授时中心原子钟的精确时间信号。

CP 证书策略 (Certificate Policy)

一套命名的规则集, 用以指明证书对一个特定团体或者具有相同安全需求的应用类型的适用性。例如, 一个特定的 CP 可以指明某类证书适用于鉴别从事机构到机构 (B-to-B) 交易活动的参与方, 针对给定价格范围内的产品和服务。

CPS 电子认证业务规则 (Certificate practice Statement)

电子认证业务规则 (Certificate practice Statement) 是关于 CA 的颁发和管理证书的运作规范描述。包括 CA 整体运行规范和证书的颁发、管理、吊

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话: 025-83393092 传真: 025-83393091

URL: <http://www.jsca.com.cn>

销和密钥以及证书更新的操作规范等事务

用户 (Subscriber)

被颁发给一个证书的证书主体。

依赖方 (Relying party)

证书的接收者，他依赖于该证书或该证书所验证的电子签名。

在本标准中，术语“证书使用者”与“依赖方”可互换使用。

私钥 (Private Key)

在公钥基础设施 PKI 中为一个密码串，由特定算法与公钥一起生成，用于解密信息或进行数字签名。在数字签名中又称为电子签名制作数据，是在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码数据。

在本标准中，术语“电子签名”与“数字签名”可互换使用。

公钥 (Public Key)

在公钥基础设施 (PKI) 中为一个密码串，由特定算法与私钥一起生成，用于加密信息或验证数字签名。在数字签名中又称为电子签名验证数据，是用于验证电子签名的数据，包括代码、口令等。

DN 惟一甄别名 (Distinguished Name)

在数字证书的主体名称域中，用来惟一标识用户的 X.500 名称。此域需要填写反映用户真实身份的、具有实际意义的、与法律不冲突的内容。

2 信息发布与信息管理

2.1 信息库

JSCA 存储用户的身份认证公开信息和证书相关信息，不包含任何交易数据，数据信息以数据库方式存放。

JSCA 通过制定数据备份和灾难恢复策略（本规范有专门章节定义）来保证存储信息的安全。

2.2 认证信息的发布

根据 X.509 标准, JSCA 在对外的目录服务器 (Directory Server) 公布证书相关信息, 并以定期和实时的方式公布证书吊销列表 CRL。

CPS 在 JSCA 网站上发布。

2.3 发布的时间或频率

JSCA 的 CRL 可以实时发布和定期发布。CPS 在改版后即更新发布。

2.4 信息库访问控制

CA 管理员可以访问 CA 数据库中的数据, RA 管理员可以访问存储在 RA 服务器数据库中的数据, 用户可以访问 JSCA 目录服务器中的数据但没有权限访问 CA 和 RA 数据库中的数据。

3 身份识别与鉴别

3.1 命名

3.1.1 名称类型

JSCA 证书体系中采用 X.500 定义的甄别名称 (DN) 标准来惟一标识一张证书的使用者的身份信息。

3.1.2 对名称意义化的要求

DN (Distinguished Name): 惟一甄别名, 在数字证书的主体名称域中, 用来惟一标识用户的 X.500 名称。此域需要填写能够反映用户真实身份的、具有实际意义的、与法律不冲突的内容。

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话: 025-83393092 传真: 025-83393091

URL: <http://www.jsca.com.cn>

3.1.3 理解不同名称形式的规则

个人证书:

名称	定义
CN 项	G + (有效证书号)
G 项	姓名
2.5.4.1	有效证书号
2.5.4.32	有效证书类型
E	邮箱
OU	内部标识 (注: 仅限数字)
2.5.4.45	证书类型
2.5.4.1111	扩展字段一
2.5.4.1112	扩展字段二
2.5.4.26	区、县
L	市
S	省
C	国家

机构证书:

名称	定义
CN	0+OU+一户口多证编号
O	机构名称
2.5.4.1	组织机构代码
2.5.4.15	工商注册号
2.5.4.31	国地税统一税务登记号
G	税务登记证号

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话: 025-83393092 传真: 025-83393091

URL: <http://www.jsca.com.cn>

E	邮箱
OU	内部标识 (注: 仅限数字)
2.5.4.13	内部编码 (注: 仅限数字)
2.5.4.45	证书类型
2.5.4.1111	扩展字段一
2.5.4.1112	扩展字段二
2.5.4.26	区、县
L	市
S	省
C	国家

3.1.4 名称的惟一性

JSCA 证书的 DN 唯一的标识一个证书用户。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

通过证书请求中包含的数字签名来证明用户持有与注册公钥对应的私钥。在 JSCA 体系中, 用户私钥 (**private key**) 在用户端生成, 用户的证书请求信息中包含用私钥进行的数字签名, CA 用对应的公钥可以验证这个签名。JSCA 要求用户妥善保管自己的私钥, 因此, 用户视作其私钥的惟一持有者。

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，JSCA 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。

JSCA 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文件，申请者需向 JSCA 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，并承担于此相关的法律责任。

JSCA 和其授权的电子认证服务机构在规定期限内保存组织机构的全部申请材料，这个规定期限由法律、政策、主管部门的要求或者 JSCA 自行决定。

数字证书登记信息发生变更时，证书持有人或证书依赖方应及时向注册机构提交变更申请。因登记信息与真实信息不符而导致的全部法律责任由证书持有人或证书依赖方自行承担。

3.2.3 个人身份的鉴别

对于个人服务使用者，RA 要验证个人的身份证件，需持个人有效身份证件，包括：身份证、军官证、士兵证、护照、武装警察身份证、户口本、港澳居民往来内地通行证、台湾居民往来内地通行证，并且需前往 RA 机构，提出申请。

数字证书登记信息发生变更，证书持有人或证书依赖方应及时向注册机构提交变更申请。因登记信息与真实信息不符而导致的全部法律责任由证书持有人或证书依赖方自行承担。

3.2.4 没有验证的用户信息

不需要验证的用户身份信息列入一个列表，表中保留已经递交过完整准确的用户信息的用户名称。

3.2.5 互操作准则

证书在和其他 CA 系统交叉认证的情况下可以和其它 PKI 系统进行互操作。因此，在证书申请中要表明证书用途。

3.3 密钥更新请求的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

JSCA 的 CA 系统需要定期在有效期即将结束时或怀疑密钥遭到攻击的情况下进行密钥更新工作。以下为 JSCA 例行密钥更新过程：

根密钥更新时，应当由全部密钥管理员在场，共同启动密钥管理程序，执行密钥更新指令，硬件加密设备重新生成根密钥。

第二层 CA 的密钥更新时，由所有密钥管理员中的多数（3 选 2）在场，共同启动密钥

管理程序，执行密钥更新指令。

对于用户，下面两种情况下要进行更新密钥对：

- 加密公钥或签名私钥已经或即将到期。
- 证书过期。
- 加密密钥对或签名密钥对已经或被怀疑受到侵害。管理员将废除的密钥对的相应证书的序列号放在 CRL 中。

3.3.2 吊销后密钥更新的标识与鉴别

证书吊销后的密钥更新操作流程等同于用户重新申请 JSCA 证书服务。

3.3.3 吊销请求的标识与鉴别

满足 4.9.1 节“证书吊销条件”的情况时，JSCA 的 RA 系统应当审核吊销申请者的申请和证书 DN 信息，在审核通过的情况下由 JSCA RA 系统来进行吊销

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

操作。

4 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

证书申请者包括具有合法身份的中华人民共和国公民、港澳台胞及在中国境内的外国公民和具有独立法人资格的企事业单位。

4.1.2 注册过程与责任

证书申请者以 JSCA 规定的方式完成认证申请表格并准备相关的身份证明材料（在申请表格中有规定）。JSCA 的 RA 或相关部门给予审核。如果申请获得批准和接受，证书可以被签发。

注册中各方责任为：RA 系统负责接收证书申请者的请求材料并在审核通过后通过安全通道传递给 CA。用户要按照 JSCA 要求准备证书申请材料并提供真实准确的信息。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

证书申请流程为：

- （1）用户到 JSCA 的 RA 递交证书申请材料；
- （2）JSCA 的 RA 对证书申请材料进行审核。

证书申请材料包括证书申请表和以下材料：

机构用户：参照 3.2.2 节的规定。

个人用户：参照 3.2.3 节的规定。

JSCA 的 RA 系统需要审查用户的证书申请表格是否按照要求填写、申请材料是否齐全、资质证明材料是否符合要求。

4.2.2 证书申请批准和拒绝

RA 根据对证书申请材料的审核的通过与否决定批准申请或拒绝发放证书。

4.2.3 处理证书申请的时间

JSCA 在收到用户的证书申请请求后应在正常工作日一天内给予处理。

4.3 证书签发

证书签发过程是：JSCA 得到 RA 通过安全方式传来的用户公开信息身份，生成证书信息并通过 RA 通知（传给用户下载证书用的密码）用户的过程。

4.3.1 证书签发中注册机构和电子认证服务机构的行为

证书发放过程中，JSCA 负责根据 RA 系统传来的用户公开身份信息，在 CA 系统中注册为用户信息。RA 负责在用户和 CA 间传输数据。

4.3.2 电子认证服务机构和注册机构对用户的通告

电子认证服务机构通过注册机构，对用户的通告有以下几种方式：

- 1) 通过面对面的方式，通知用户本人到注册机构领取数字证书；注册机构把证书等直接提交给用户；
- 2) 邮政信函通知用户；
- 3) 其他 JSCA 认为安全可行的方式通知用户。

4.4 证书接受

4.4.1 构成接受证书的行为

在 JSCA 数字证书签发完成后，申请者至 JSCA 网点领取，证书申请者从获得证书起就被视为已同意接受证书。证书申请者接受数字证书后，应妥善保管其证书对应的私有密钥和承载证书的介质。

4.4.2 电子认证服务机构对证书的发布

江苏在签发完证书后，将把证书及公钥信息发布到 JSCA 系统的目录服务器中，供用户和依赖方查询和下载。

4.4.3 电子认证服务机构对其他实体的通告

证书申请成功后，是否可以信任，其他用户可以在 CA 目录服务器中查到。

4.5 密钥对和证书的使用

4.5.1 用户私钥和证书的使用

用户需要妥善保管自己的私钥和证书，不得将其用于不适合的证书用途（在 1.4.2 节定义），也不可在证书已过期或被吊销的情况下继续使用证书和密钥。

4.5.2 依赖方公钥和证书的使用

依赖方有义务妥善保管用户的公钥和证书，不将其用于不适合的证书用途，使用前有责任根据 CPS 的规定检查证书的有效性。

4.6 证书更新

4.6.1 证书更新的情形

证书更新指 JSCA 在不修改证书中的用户相关公开身份信息的情况下重新生成一张证书。

4.6.2 请求证书更新的实体

由 JSCA 或授权机构颁发的原有证书有效期限未到的个人、单位、服务器、机构、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 JSCA 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

申请者到 JSCA 或授权的发证机构书面填写《江苏省数字证书业务申请单》进行办理；JSCA 或授权的发证机构按照身份标识与鉴别办法对用户提交的证书更新申请进行审核；新证书签发后，旧的证书将被注销。CA 中心将在 2 小时内 LDAP 上发布用户的新证书。用户旧证书废止信息在 24 小时内通过 CRL 发布。

4.6.4 颁发新证书时对用户的通告

电子认证服务机构通过注册机构，对用户的通告有以下几种方式：

- 1) 通过面对面的方式，通知用户本人到注册机构领取数字证书；
- 2) 注册机构把证书等直接提交给用户；
- 3) 邮政信函通知用户；
- 4) 其他 JSCA 认为安全可行的方式通知用户。

4.6.5 构成接受更新证书的行为

以下步骤构成接受更新证书的行为：

- 1) 人工方式下，JSCA 的 RA 执行证书更新操作；
- 2) JSCA 根据 X.509 标准用户的公开身份信息组成新的证书信息；
- 3) 用户进行证书更新。

4.6.6 电子认证服务机构对更新证书的发布

JSCA 在签发更新证书后，就将更新证书发布到目录服务器中，对外进行发布。

4.6.7 电子认证服务机构对其他实体的通告

关于该证书是否可以正常使用，其它用户可以在 JSCA 的对外的目录服务器上查到。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

证书密钥更新条件具体包括：

- 用户忘记了证书使用密码。
- 用户证书和密钥对到期
- 用户证书（文件）丢失或损坏，例如存放证书的介质损坏。
- 用户认为原有证书已不安全，例如客户怀疑证书被盗用或密钥受到了攻击。

4.7.2 请求证书密钥更新的实体

证书更新申请者为 JSCA 证书用户。

4.7.3 证书密钥更新请求的处理

JSCA 证书用户向 JSCA 的 RA 递交证书密钥更新请求，由 RA 审核用户的申请材料。

4.7.4 颁发新证书时对用户的通告

通过面对面的方式，通知用户本人到注册机构领取数字证书；或注册机构把证书等直接提交给用户；或使用邮政信函通知用户；或其他 JSCA 认为安全可行的方式通知用户。

4.7.5 构成接受密钥更新证书的行为

以下步骤构成接受密钥更新证书的行为：

- (1) JSCA 的 RA 执行证书密钥更新操作；
- (2) JSCA 根据 X.509 标准用户的公开身份信息组成新的证书信息，生成新密钥；

4.7.6 电子认证服务机构对密钥更新证书的发布

JSCA 在签发更新证书后，就将跟新证书发布到数据库和目录服务器中，对外进行发布。

4.7.7 电子认证服务机构对其他实体的通告

关于该证书是否可以正常使用，其它用户可以在 JSCA 的对外的目录服务器上查到。

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

4.8 证书变更

4.8.1 证书变更的情形

证书变更指改变证书中除用户公钥之外的信息而签发新证书的情形。当用户实体身份信息发生改变，而影响证书项内容时，JSCA 证书用户可以向 JSCA 申请证书变更。

4.8.2 请求证书变更的实体

证书更新申请者为用户状态为活动的 JSCA 证书用户。

4.8.3 证书变更请求的处理

处理步骤为：

- (1) 由证书持有者本人持有效证件到申请证书的分支机构 LRA 提出证书修改请求；
- (2) LRA 对有效证件进行审核；
- (3) 审核通过后在 RA 服务器的数据库中根据客户信息进行查询；
- (4) RA 修改本地审核数据库中的记录并发给 CA 证书数据库。

4.8.4 颁发新证书时对用户的通告

申请证书变更的用户可以在向 JSCA 成功提交证书申请后，凭证书申请表领取电子认证证书。证书领取时间详见各对应的证书变更申请表。用户在领取后，请详细查看证书及其内容，如有问题可以在 7 个工作日之内与 JSCA 联系解决。

4.8.5 构成接受变更证书的行为

以下步骤构成接受变更证书的行为：

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

JSCA 根据用户修改后的公开身份信息按照 X.509 标准生成新证书。

4.8.6 电子认证服务机构对变更证书的发布

JSCA 通过 LDAP 证书库的方式公开发布变更后的证书，同时在 JSCA 网站（www.jsca.com.cn）提供变更证书查询服务 LDAP 的地址（58.213.155.115 根节点 o=jsca）查询变更后的证书信息。

4.8.7 电子认证服务机构对其他实体的通告

关于该证书是否可以正常使用，其它用户可以在 JSCA 的对外的目录服务器上查到。

4.9 证书吊销和挂起

以下对证书吊销和挂起的情况进行描述。

4.9.1 证书吊销的情形

对于下列情况之一，JSCA 将吊销所签发的数字证书：

- 1) 用户申请数字证书时，提供的资料不真实；
- 2) 用户没有按照规定缴纳数字证书服务费用；
- 3) 用户未履行证书服务责任书约定的义务；
- 4) 用户要求吊销数字证书；
- 5) 用户主体消亡；
- 6) 用户变更数字证书的用途；
- 7) 其他情况。这些情况可以是因法律或法规的要求，JSCA 采取的吊销措施。
- 8) 吊销分为主动吊销和被动吊销。主动吊销是指由用户提出吊销申请，由 RA 或 RA 受理点 LRA 进行审核并由具有相关权限的操作员对其要求进行处理，吊销证书；被动吊销是指当 RA 确认用户违反证书应用规定或已经消亡等情

况发生时，采取吊销证书的手段以停止对该证书的证明。

4.9.2 请求证书吊销的实体

可以要求证书吊销的实体有最终用户和 RA。

4.9.3 吊销请求的流程

RA 系统强制吊销是由 RA 管理员根据 CA 策略对终端用户的证书执行吊销操作；终端用户申请吊销是用户向 RA 系统提出申请，并由 RA 系统审核，审核通过后，吊销该用户证书。

4.9.4 吊销请求宽限期

RA 强制吊销可以给予 24 小时的宽限期。终端用户申请吊销时，RA 应在收到吊销请求后立即吊销证书，没有宽限期。

4.9.5 电子认证服务机构处理吊销请求的时限

CA 在接到吊销请求后应立即处理且在 24 小时内完成。电子认证服务机构证书的证书撤销列表（CRL），至少每年签发一次。

4.9.6 依赖方检查证书吊销的要求

依赖方需要访问 JSCA CRL 服务器来查询用户的证书状态，以获得用户证书是否可以信赖的信息。

4.9.7 CRL 发布频率

JSCA 每 12 小时更新一次 CRL。

4.9.8 CRL 发布的最大滞后时间

CRL 发布的最大滞后时间为 24 小时。

4.9.9 在线的吊销/状态查询的可用性

使用 JSCA 提供 7X24 小时 CRL 目录服务，可以进行证书吊销查询和状态查询。

4.9.10 在线的吊销查询要求

依赖方通过查询 JSCA (CRL) 来判断证书是否可信。

4.9.11 吊销信息的其他发布形式

暂未提供 OCSP 服务。

4.9.12 对密钥遭攻击的特别处理要求

在 JSCA 的 CA 证书和密钥遭到攻击的情况下，JSCA 颁发的证书均需要吊销。

4.9.13 证书挂起的情形

以下情况出现时考虑证书挂起：

- (1) 用户怀疑证书或密钥受到攻击。
- (2) 用户的资信暂时出现问题或无法证明其资信。
- (3) 没有按期缴纳证书费。

4.9.14 请求证书挂起的实体

RA 和用户状态为活动的 JSCA 证书用户

4.9.15 挂起请求的流程

终端用户的证书挂起分为 RA 强制挂起和终端用户申请挂起。RA 强制挂起是由 RA 管理员根据 CA 策略将终端用户的证书进行挂起操作；终端用户申请挂起是用户提出申请，并由 RA 审核，审核通过后，挂起该用户证书。

4.9.16 挂起的期限限制

证书挂起的期限在 CA 中设置，挂起期间，被挂起证书无法用于正常的证书应用。

4.10 证书状态服务

4.10.1 操作特征

JSCA 开放目录服务器为用户提供证书状态服务。目录服务器是证书管理和证书应用的关键环节。JSCA 的目录服务器系统采用 LDAP 协议（LDAP: Lightweight Directory Access Protocol, 轻型目录存取协议，符合 RFC 1777 规范要求。协议特点：以树状的层次结构来存储数据和适用于读密集型操作），将证书和证书吊销列表(CRL)存放在其中供应用需要在需要验证身份时查询。

JSCA 选用功能完善、性能良好的目录服务器产品，采用的是单个主目录、多级和同级多个镜像目录器部署的结构。主目录服务器处于最安全区，仅和 CA 系统相连。根据需要在一些地方建立镜像目录服务器，由 JSCA 定期将主目录服务器的内容发布到镜像目录服务器，直接面向证书用户。

4.10.2 服务可用性

这项服务在 JSCA 停止服务之前将一直向用户开放。采用高性能和高可用性的设备和系统，提供 7X24 小时不间断服务。

4.10.3 可选特征

当用户的证书使用中遇到问题的情况下，可以由 JSCA，查询 CA 数据库中证书用户的状态并将之通知用户。

4.11 订购结束

用户声明不使用 JSCA 证书服务的情况下，JSCA 的 RA 可以在系统中注销该用户和相关该用户的证书有关信息，并发布证书作废消息。

4.12 密钥生成、备份与恢复

4.12.1 密钥生成、备份与恢复的策略与行为

具体的策略与行为在本文 6.1 节和 6.2 节描述，密钥也可以由可信的第三方的符合国家安全管理要求的密码模块（例如加密机）产生、备份与恢复。

4.12.2 会话密钥封装和恢复策略与行为

用非对称算法封装会话密钥，可以用解密密钥来解开并恢复会话密钥。

5 认证机构设施、管理和操作控制

5.1 场地位置与建筑

JSCA 主机房位于江苏省委内，分为三层安全级别，其中第一层、第二层和江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

管理机房的物理通道。JSCA 还将在公司以外的地区建立异地备份中心。所有机房的建设和管理严格按归国家有关规定要求，采用高安全性的监控技术，包括初步实现监控、指纹仪、身份识别卡等监控技术，以确保物理通道的安全。机房内部禁止拍照、摄像，只有经过 JSCA 制空权的人员才能进入授权的部门和地点。

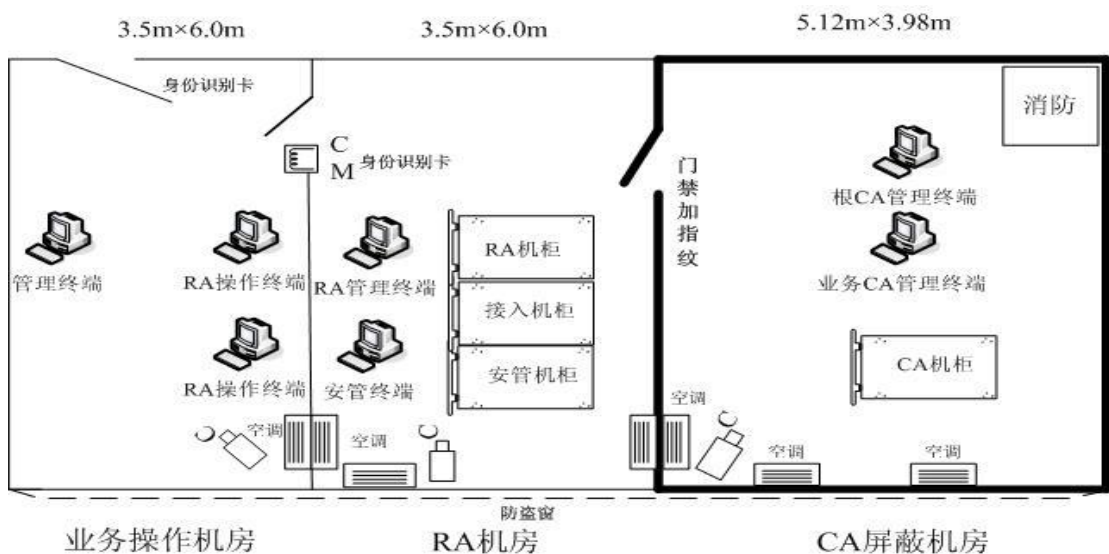
5.1.1 物理访问

在江苏省数字证书认证系统的物理建设中，严格按照分层建设、多级管理的要求实施机房布局。建设过程中将每一个层次建设为一道积极的屏障，如锁着的门或关闭的大门，它可以对个人的进入提供强制性的控制；门禁系统设立办公区及大门门禁，对于人员的可出入区域根据工作性质、权限进行严格划分。在员工离职或丢失了磁卡时立即删除权限和记录。安全区机房采用双指纹多层门禁系统，每个工作室都安装电子出入控制系统、防侵入系统、机械组合锁等装置。并且每个人要进入下一个区域，必须做出积极的反应（例如，门开锁或大门打开）。

在江苏省数字证书认证系统机房，物理系统分为 3 层结构，如图所示：

- 第一层为 CA 的 DMZ 区。
- 第二层为 RA 管理员的操作区域和权限管理区域。
- 第三层为 CA 系统机房，属于证书签发区域。

CA 机房结构图



江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

5.1.2 电力与空调

为了保证系统的正常运行，防止由于断电产生的灾难性后果，系统配置了美国 BEST POWER 不间断电源系统。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，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，采用海尔三菱空调控制室温湿度。

5.1.3 水患防治

JSCA 机房的排水系统作为防水设施。

5.1.4 火灾防护

符合现行国家有关消防标准规范，为保障建筑内部装修的消防安全，贯彻“预防为主，防消结合”的消防工作方针，防止和减少建筑物火灾的危害。

机房消防报警系统采用美国爱德华智能消防报警系统。系统通过设置在机房的温感和烟感采集消防数据，同时该系统实时处理用户火灾自动报警终端的报警数据和系统运行状态数据。系统管理分手动模式和自动模式两种，实现网络系统实时检测、监测和系统的手动、自动控制模式的设定，并完成了系统设计的有关各种联动动作。省密钥管理中心消防报警系统建设根据《卤代烷 1211 灭火系统设计规范(GBJ 110-87)》，该设备清洁、低毒，对保护对象没有损害，具有其他各类灭火设备不可比拟的优点，是目前应用最广泛的气体灭火设备。

5.1.5 介质存储

存储介质必须得到安全可行的保护，温度、湿度、磁力等环境变化可能产生的危害和破坏。具体要求在 MSCA 技术标准和规程中做出了具体规定。

5.1.6 废物处理

废弃物的处理：纸介质用碎纸机粉碎或焚毁，其他介质以不可恢复原则进行相应的销毁处理。

5.1.7 异地备份

为保证数据的完整性与可恢复性，制定备份策略，在异地建立备份中心，存储JSCA运行系统的备份数据和介质。

本策略确定的备份指对CA系统的备份，具体有正式系统的三层CA及目录服务、前置机、网站、加密机、CA、数据库等核心数据的备份。根据数据重要性和备份的复杂程度安排日常备份和阶段性备份。日常备份采用每日、每周手工保存备份数据的压缩包到硬盘或光盘备份。阶段性备份是在日常备份的基础上为了较长时间的保存数据，采用的通常以月、季度或者半年为时间单位的备份。操作上，采用手工备份数据到光盘上的方式。

备份由技术部人员和安全部人员共同负责。

5.2 程序控制

5.2.1 可信角色

系统角色包括系统管理员、系统操作员和审核员等。

5.2.2 每项任务需要的人数

对于可信任角色，系统规定其权限，对于任务，系统规定参加的角色和人数。系统管理员具有完成所有功能的权利，并负责管理操作员的建立和口令。系统管理员设置两名，他们的口令绝对保密，身份认证的方式也必须很严格。对系统管理员的操作进行日志记录，以进行审计跟踪。系统操作员的权限受到限制，只能执行一般的操作，不能建立用户，无权改变系统设置。在进入系统时，必须通过江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

权限设置或身份认证。审核员对操作员的操作进行审核。系统对系统操作员的操作进行日志记录，以进行审计跟踪。

5.2.3 每个角色的识别与鉴别

使用数字认证和PIN口令对可信角色进行身份认证。

5.2.4 需要职责分割的角色

系统规定不能由同一人担任不同的角色以便进行角色和职责的分割。

5.3 人员控制

5.3.1 资格、经历和无过失要求

JSCA对运行人员的背景、资历、经验等情况都进行核实和审查。至少必须具备诚信度、忠实度及工作的热诚度、无影响CA运行的其它兼职工作、无同行业重大错误记录、无违法记录等。

5.3.2 背景审查程序

JSCA 员工的录取经过严格的审查，根据岗位需要增加相应可信任的员工。一般员工需要有 1-3 个月的考察期。根据考察的结果安排相应的工作或者辞退。JSCA 根据需要对员工进行职责、岗位、技术、政策、法律、安全等方面的培训。

JSCA 会对其关键的 CA 职员进行严格的背景调查。受理点责任单位可以在此基础上，增加考察和培训条款，但不得违背 JSCA 证书受理的堆积和 JSCA 认证业务声明。

JSCA确立流程管理规则，据此CA员工受到合同和章程的约束，不许泄露JSCA证书服务体系的敏感信息。所有的员工与JSCA签订保密协议，合同期满以后3年内仍然不得从事与JSCA相类似的工作，报第三方公证。

5.3.3 培训要求

JSCA 对员工进行以下内容的综合培训：

- JSCA 安全原则和机制；
- JSCA 使用的软件介绍；
- JSCA 操作的系统和网络；
- JSCA 质量控制体系；
- 岗位职责；
- JSCA 政策、标准和程序；
- 相关法律、仲裁规则、管理办法等。

5.3.4 再培训周期和要求

根据JSCA策略调整、系统更新等情况，JSCA将对员工进行继续培训，以适应新的变化。

5.3.5 工作岗位轮换周期和顺序

JSCA提供7X24小时不间断服务，有合理的轮班制度。运行部门按照人员和工作计划排定轮班，使得在不影响工作的情况下合理安排运行人员的工作和休息，提高工作效率。运行部门将运行人员进行排班，要求管理系统的运行，记录运行情况，在下一班到岗前不得离开岗位。

5.3.6 未授权行为的处罚

当 JSCA 员工进行了未授权或越权操作，JSCA 在确认后立即中止该员工进入 JSCA 证书服务体系。根据情节严重程度，实施包括提交司法机关处理等措施。

5.3.7 独立合约人的要求

安全方面，对于合同工的要求和对于正式工的要求是一样的。不安排其接触系统核心软/硬件及网络设施并对其按照合同进行审计和监察。

5.3.8 提供给员工的文档

为使得系统正常运行，必须提供给具有权限的相关人员各种文档，这些文档包括：

- 软/硬件、网络设备安全操作手册
- 加密机、密钥管理安全操作手册
- RA 系统相关安全操作手册
- JSCA运行策略、运行规范
- 系统备份与恢复安全操作规范和手册等其他文档。

5.3.9 关键岗位人员离职

针对密钥管理员离职、换岗的情况，制定了密码口令和相关载体的安全处理规定。

5.4 审计日志程序

各运营CA 的审计日志由运行部门和技术部门统一保存，每天定期备份，备份介质分别存放在JSCA与异地备份中心，存放期5年。一旦出现审计纠纷，需要对审计日志提出复查，应由客户报市场部，经总经理同意后，由运行人员查询。

5.4.1 记录事件的类型

记录的种类包括：

- 对物理与环境安全的审计，通过定期根据安全策略，检查相关设施来实

现。

- 对网络安全的审计，是利用相应的安全措施定期对网络进行测试，以检测是否出错。
- 证书处理系统应用与数据的安全审计，可采用定期对其有关重要操作的审计尾迹分析来进行。
- 定期对人员行为的原始记录进行分析，达到人员审计的目的。
- 定期对整个系统从物理与环境、网络、数据和人员等方面进行检测，实现对系统的审计。
- 使用操作系统本身提供的各种日志文件，记录操作系统一级的各种日志，包括用户登录、FTP 连接、Telnet 连接，以及系统提供的历史记录等。通过查看这些日志文件，可以发现异常情况和试图非授权使用系统功能的痕迹。
- 数据库审计是使用数据库系统提供操作审计功能，以一种比较安全的方式记录下需要跟踪的操作，然后提供给数据库审计人员进行审计和跟踪。
- 通过配置需要跟踪审计的内容（如对什么人进行什么操作进行记录等）形成相应的配置文件，然后启动审计程序，产生一个带有时间戳标记的不可读也不可修改的日志文件。审计人员通过系统提供的转换工具可将该文件转换成可读的文本文件，通过该文本文件，审计人员就可跟踪查看所有的操作记录。
- CA 系统软件专门设有监控系统，各服务器在运行过程中将其运行状况通过发送给监控系统，包括服务器启动、停止等运行状态，以及系统运行过程中的业务数据处理信息，如请求包类型、状态、处理情况等。这样，通过监控系统，就可实时了解到系统各服务器运行状况，用于对整个CA 系统进行监控和维护。
- CA 系统软件处理设置监控系统外，每个服务器都对执行的各种操作进行了详细的日志记录。这些记录包括服务器本身的启动和关闭，操作员的证书序号、所执行的操作，系统接收到的各种数据包、所作的处理、

处理结果，系统运行过程中的出错、异常等。根据这些日志记录，系统审计员可以执行对操作员的操作审计、证书管理事件审计和密钥管理事件审计。

5.4.2 处理日志的周期

每周至少进行一次审计跟踪处理(检查违反政策及其他重大事件)。在报警或异常事件发生后也要处理日志。

5.4.3 审计日志的保存期限

密钥、证书信息档案和审计跟踪文档至少保留五年以上。

5.4.4 审计日志的保护

审计人员才可以浏览审计日志，审计日志无法更改和删除。

5.4.5 审计日志备份程序

所有审计日志由运行部门专人每天备份，存放在专门的硬盘或光盘库中，同时定期备份数据文件，存放到异地备份中心。

5.4.6 审计收集系统

由CA 和RA 系统以及CA 和RA 管理员完成。方式上有系统自动和人工采集方式。

5.4.7 对导致事件实体的通告

如发生事故应立即通知相关的事故责任人和系统管理员。

5.4.8 脆弱性评估

对于可能对CA系统的侵害，需要由CA运行部门进行脆弱性评估，以便将系统运行的风险降至最低。每年至少执行一次。

5.5 记录归档

日志纪录由系统定期归档，由运行人员每天复查，每周由运行人员进行有效性验证，以检查归档记录是否可用。

5.5.1 归档记录的类型

JSCA对审计数据、证书用户公开身份信息、CA系统数据和目录服务数据、密钥历史等记录归档保存。

5.5.2 归档记录的保存期限

CA数据库的保存期至少为十年。审计跟踪文档要至少保存五年。

5.5.3 归档文件的保存方式

归档保存在三个地点，系统硬盘保存一份，备份光盘库保存一份，异地备份中心保存一份，备份保存在有安全控制的房间内，要求在防潮湿、防静电感应的中央空调环境下。没有授权的人员无法访问和更改。为防止介质老化，周期性将数据保存到新的介质上。。

5.5.4 归档文件的备份程序

根据数据重要性和备份的复杂程度安排日常备份和阶段性备份。日常备份采用每日、每周手工保存备份数据的压缩包到硬盘或光盘上备份。阶段性备份是在日常备份的基础上为了较长时间的保存数据，采用的通常以月、季度或者半年为

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路10号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

时间单位的备份。操作上，采用手工备份数据到光盘上的方式。此外，在对系统进行变更前也应该采用阶段性备份的方式，用于较长时间的保存备份成果。

备份由技术部和安全部门人员共同负责。

5.5.5 记录时间戳要求

归档的记录都需要标注标准北京时间。

5.5.6 归档收集系统

系统以命令脚本的方式控制归档内容。

5.5.7 获得和检验归档信息的程序

归档的信息的两个拷贝由两个管理员分别管理，通过对比两个拷贝来判断归档信息是否准确。

5.6 电子认证服务机构密钥更替

在CA 的密钥对遭受攻击或因为密钥生命期而需要更新密钥对的情况下，参照3.3.1节相关内容进行密钥更换。

5.7 损害与灾难恢复

CA系统的灾难恢复，指的是为保证在发生灾害（水灾、风灾、地震等自然灾害，或电力中断、火灾、爆炸等结构性破坏以及人为失误、网络黑客攻击、病毒等操作问题）或战争等攻击而导致CA 彻底损毁时，能够恢复CA 的密钥和该CA 的用户资料。

通过在异地设立灾备份中心可以实现灾难恢复。灾备份中心存放各级CA 的备用设备，该加密机中的私钥与运行系统的私钥相同。CA 中心在更新密钥时同时更新备用加密机中的密钥。同时，根CA 还必须定期将系统备份服务器

江苏省电子商务证书认证中心有限责任公司
南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

中的数据通过磁盘备份，以人工方式送到异地容灾备份中心。当公钥基础设施（PKI）发生灾难性故障时，JSCA拥有恢复运营的能力。首先是确定灾难恢复的重要性以及恢复PKI运行的可接受时间。它们是确定PKI是否需要一个全面冗余灾难恢复（DR）站点的关键因素。

灾难恢复的具体工作包括：

- 制定灾难恢复计划；
- 数据的备份和存储；
- 辅助设备准备；
- 启动灾难恢复计划；
- 灾难恢复所需时间评估。

5.7.1 事故和损害处理程序

流程为：

1. 保证现有的对外提供的所有设备能够正常提供服务，并且针对每个环节设置紧急预案。
2. 所有对外服务的设备都具备基本的监控
3. 出现故障时，应以尽快正常对外提供服务为目标，记录故障现场。
4. 对于影响面大的故障，发现问题半小时内不能快速解决问题的，应考虑启动紧急预案。
5. 严重影响对外服务的故障，应该及时上报主管领导。

5.7.2 计算资源、软件或数据的损坏

当计算资源、软件或数据受到破坏后，进行以下操作：

- （1）恢复环境，启动备份系统和备份数据并上线；
- （2）为用户恢复证书。重新进行认证。
- （3）尽快恢复原系统。

5.7.3 实体私钥损害处理程序

参照本文相关章节进行证书密钥更新。

5.7.4 灾难后的业务连续性能力

灾难发生后JSCA 立即用备用系统上线对用户提供服务，保持业务持续性。

5.8 电子认证服务机构或注册机构的终止

CA 和 RA 应该提前 90 天向所有未吊销或未过期证书的用户发布即将终止 CA 和 RA 的信息，在此期间内停止使用该 CA 或 RA 所发放的证书。CA 应当在终止服务 60 日前向工业和信息化部报告，并与其他 CA 就业务承接进行协商。如果未能就业务承接事项与其他 CA 达成协议的，应当申请工业和信息化部安排其他电子认证服务机构承接其业务。

对于CA终止步骤为：

- 上报认证中心主管；
- 收回证书；
- 整理存档记录；
- 停止认证中心所有业务；
- 主目录服务器存档；
- 关闭主目录服务器；
- 关闭备份目录服务器；
- 销毁密钥；
- 存储重要信息；
- 清理认证中心硬盘、光盘库；
- 在最后终止CA 的服务前，要取消所有由JSCA发布的证书。

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

根CA: 根CA 的根密钥对由硬件加密设备直接产生, 并且直接保存在该硬件加密设备中, JSCA使用的是国家商业密码管理委员会鉴定通过的加密硬件设备。产生密钥的时候, 必须由三个密钥管理员同时登录后由加密硬件设备产生, 任何单独的一个人均没有办法执行产生密钥的操作。密钥管理员登录是采用IC 卡的方式, 其他人员无法获知IC 卡或相应的密码。

业务CA: 拥有的加密密钥对由根CA 的加密机产生, 签名密钥对在本地硬件加密设备上产生, 私钥不能出此加密硬件设备。产生密钥的时候, 必须由三个密钥管理员中的多数同时登录后由加密硬件设备产生, 任何单独的一个人没有办法执行产生密钥的操作。密钥管理员登录是采用IC 卡的方式, 其他人员无法获知IC 卡或相应的密码。

用户: 签名密钥对在客户端产生, 具有严密且安全的控制措施, 可采用智能IC 卡、其它硬件加密设备或加密软件生成。

6.1.2 私钥传送给用户

加密私钥由KMC 生成, 签名私钥由存储介质生成。

6.1.3 公钥传送给证书签发机构

JSCA 的根公钥包含在 JSCA 自签发的根证书中。 JSCA 中心支持在线传递公钥或从 JSCA 的网站下载 JSCA 根证书和 CA 机构的证书。

6.1.4 电子认证服务机构公钥传送给依赖方

CA 会把自己的公钥通过安全软件或建立的安全通道发给依赖方以便依赖方可以用来加密发给 JSCA 的信息。

6.1.5 密钥的长度

JSCA 非对称密钥对采用密钥长度为 1024 位的 RSA 算法。

6.1.6 公钥参数的生成和质量检查

系统使用 PKI 密钥生成算法生成随机数作为公钥参数，判断根据该公钥参数是否产生破解难度小的弱密钥。如果是则抛弃会产生弱密钥的公钥参数。

6.1.7 密钥使用目的

密钥用途有多种，在证书的“密钥用途”域中有定义，主要分为加密、解密、签名和验证等几种用途。

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

密码模块采用 56 所生产的加密机，安置在安全区。并在有至少两名管理员在的情况下才可以访问存储在加密机中的密钥。加密机的数据包括两方面的内容：管理员口令卡、CA 私钥的备份。备份与恢复加密机必须同时拥有三张管理员口令卡片，才能对加密机进行备份与恢复的操作。

根据以上的特点规定：

(1) 线上的加密机，无论是运行着的还是冷备份的，必须将 CA 私钥的备份文件删除；

(2) 管理员口令卡片由安全主管负责掌握，一旦需要使用，必须经过技术部负责人与安全主管共同申请，由总经理签字方能使用。使用时必须由运维部负责人在场，不得随意复制，使用后交还安全主管保管，使用前后必须登记。

CA根 私钥的备份数据以IC卡形式存放在保险柜中，如有特殊情况需要使用，必须经技术部门负责人与安全主管共同申请，由总经理签字。

6.2.2 私钥多人控制 (m 选 n)

激活、备份、恢复私钥实施了M选N多人控制 ($M > N > 1$)，并记录操作过程。

6.2.3 私钥托管

作为灾难恢复的一项措施，需要进行密钥托管。密钥托管的情况下，私钥以分段加密的方式存储在加密机中，需要在有管理员中的大多数同时在场的情况下才可以起用私钥。

加密私钥由KMC进行密钥托管，JSCA不托管用户的签名私钥。

6.2.4 私钥备份

作为灾难恢复的一项措施，需要进行根密钥备份。JSCA采用五十六所研制的加密主机对CA根私钥进行加密和备份，备份存储在与系统独立的系统内防止被窃。在备份密钥时，必须由密钥管理员使用加密IC卡，启动密钥管理程序，执行密钥备份指令才能完成。用户签名私钥无法备份。

6.2.5 私钥归档

作为灾难恢复的一项措施，需要进行密钥归档。不再使用的私钥，由运维部人员操作，将密钥以分段加密的方式归档，需要多管理员同时在场才可以恢复私钥。

6.2.6 私钥导入、导出密码模块

CA新密钥对产生时，需要备份并向加密机输入私钥。当需要恢复私钥时，需要将加密机中的私钥输出。以上操作都有两名以上运行部人员参加，密钥以分段加密的方式存储在加密机中。

6.2.7 私钥在密码模块的存储

加密机中私钥分段加密存放，这样由多个管理员每人掌握其中一段密钥的解密密码，增强了密钥管理的安全性。

6.2.8 激活私钥的方法

具有激活私钥权限的技术部管理员使用含有自己身份的加密IC卡登录，启动密钥管理程序，进行激活私钥的操作，需要多管理员同时在场。

6.2.9 解除私钥激活状态的方法

具有冻结私钥权限的运维部管理员使用含有自己的身份的加密IC卡登录，启动密钥管理程序，进行冻结私钥的操作，需要多管理员同时在场。

6.2.10 销毁私钥的方法

在 JSCA 证书服务体系中作废私钥采取以下形式：

- 存取私钥的介质被损坏或丢失
- 向 JSCA 或受理点归还私钥
- 旧密钥对被新的密钥对取代
- JSCA 执行过期数据处理程序

6.2.11 密码模块的评估

JSCA使用的加密机是五十六所研制，并通过国家密码管理委员会办公室鉴定并批准使用的具有自主知识产权的高速主机加密设备。该系列利用加密和数字签名技术保证用户在网上传递信息的机密性（即数据在传输过程中不能被非授权者窃取）、完整性（即数据在传输过程中不能被非法篡改）和有效性（即数据不可被否认），构建一个电子商务正常发展所必需的安全环境和信用环境。产品特点：

- （1）功能完备，集密钥管理、数据加密、数字签名、完整性检验于一体；
- （2）使用IC卡保存PIN，设置密钥管理员和操作员，密钥管理实行分割管理和权限控制；
- （3）安全密钥管理，密钥不以明文形式出现在磁盘及内存中，即使受到攻击，也能保证密钥的安全。
- （4）支持RSA、DSA、ECC、SF33、Diffe Hellman等公钥算法，RSA模长可选512、768、1024比特；
- （5）支持DES、3DES5等对称算法，支持128 比特高强度加密，
- （6）支持MD2、MD5、SHA1、SDHI等HASH算法；
- （7）提供PKCS#7、X.509等国际标准开发接口；
- （8）支持Windows等操作环境；
- （9）和主机的连接方式支持TCP/IP或并口；
- （10）高可靠性，双机备份，容错。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

由管理员操作证书和公钥的归档。

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，但并不完全保持一致。对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名。但是为了保证在证书有效期内签名信息被验证，公钥的使用期可以在证书的有效期外。对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息。但是为了保证在证书有效期内加密信息被解开，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取以上情况的最大值。

除 JSCA 特殊声明的情况以外，JSCA 对密钥对的使用期限没有特定的要求，只要在 CA 终止前使用即可。

6.4 激活数据

6.4.1 激活数据的产生和安装

激活数据是私钥保护密码，指用户用于使用私钥的密码，由用户自己产生并且需要符合一定的安全策略。例如至少6位字节长、需要在密码中同时具有大小写字符和数字等。

6.4.2 激活数据的保护

激活数据可以以字符串等方式存在。用户需要进行妥善保护不要泄露给其他人，如果因为激活数据丢失造成的私钥被盗用进行操作的情况，将视同私钥主人用私钥进行操作。

6.4.3 激活数据的其他方面

私钥保护密码在使用中可以修改以提高其安全性。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

JSCA的系统在安全的环境下运行，并实行分安全区访问权限控制。核心系统和其它系统隔离，采用防火墙和入侵检测保证安全。并实行：

1. 系统安全配置，关闭不必要的服务与端口。
2. 操作系统必须安装最新的补丁程序，由专人负责最新补丁的安装。
3. 生产系统每台机器均由专人负责，严格上机操作程序，口令逐级管理，逐级授权。
4. 各人负责各自权限范围内的操作。
5. 日志和操作记录的审计制度。
6. 数据备份和恢复机制。

6.5.2 计算机安全评估

系统安全等级采用内部规定标准执行。

6.6 网络的安全控制

根据安全要求的不同，将JSCA系统划分为不同的网段，部分高安全级系统进行离线操作。并采用层次模型保证网络的安全性以及系统的可靠性，具体体现为以下几个方面：

- 第一：路由器实施对来自外部的访问信息过滤控制。
- 第二：采用多层次防火墙结构，所有从外部对JSCA的访问，都受到防火墙安全体系控制。
- 第三：将功能独立的服务器放置在不同的网段。
- 第四：通过对验证和存取访问权限控制进行保护。
- 第五：在应为JSCA网络系统中，采用网络安全管理产品，从检测与监听等多方

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

面对网络系统进
行防护，及时发现入侵者并报警，并实施事件响应。
第六：提供系统冗余设计。

6.7 时间戳

JSCA系统的系统数据和日志记录等均可以根据标准时间源的时间戳记录，以作为审计之用。时间戳系统提供的时间戳服务在技术实现上严格遵循国际标准时间戳协议（RFC3161），采用标准的时间戳请求、时间戳应答以及时间戳编码格式，时间源采用国家授时中心提供的标准时间。

7 证书、证书吊销列表和在线证书状态协议

7.1 证书

7.1.1 版本号

JSCA 证书由广泛的通用性。证书格式符合 X.509: V3 标准。

7.1.2 算法对象标识符

算法：

非对称算法：RSA(512、1024、2048 位)，ECC、DSA、Diffie、Hellman。

对称算法：DES、3DES、CAST、SDBI、IDEA、RC2、RC4、RC5。

签名/摘要算法：MD2、MD5、SHA1。

7.1.3 名称形式

个人证书：

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

名称	定义
CN 项	G + (有效证书号)
G 项	姓名
2.5.4.1	有效证书号
2.5.4.32	有效证书类型
E	邮箱
OU	内部标识 (注: 仅限数字)
2.5.4.45	证书类型
2.5.4.1111	扩展字段一
2.5.4.1112	扩展字段二
2.5.4.26	区、县
L	市
S	省
C	国家

机构证书:

名称	定义
CN	0+OU+一户口多证编号
O	企业名称
2.5.4.1	组织机构代码
2.5.4.15	工商注册号
2.5.4.31	国地税统一税务登记号
G	税务登记证号
E	邮箱
OU	内部标识 (注: 仅限数字)

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话: 025-83393092 传真: 025-83393091

URL: <http://www.jsca.com.cn>

2.5.4.13	内部编码 (注: 仅限数字)
2.5.4.45	证书类型
2.5.4.1111	扩展字段一
2.5.4.1112	扩展字段二
2.5.4.26	区、县
L	市
S	省
C	国家

注:

(1) JSCA 要求, 证书主题项的排列顺序从前到后依次为: CN、G、E、OU、O、L、S、C

(2)、WWW 服务器证书中的 CN 内容为域名或 IP 地址。

7.1.4 名称限制

在 DN 中, 可以使用除专用字符和特殊字符外的所有 ASCII 字符。专用字符为反斜杠("\")和双引号(""), 由于在 DN 中有特殊含义, 不能在 DN 中。另外, 如果在 CN 中包含特殊字符(", ", "=", "+", "#", "<", ">", "; "), JSCA 系统会做特殊处理, 即对整个 CN 内容加双引号, 这样会导致以后实际处理上的不方便, 因此不允许在 CN 中包含这些特殊字符。

由于存在不可见的 ASCII 字符, 不便于用户使用, 下面给出本标准中所有可用的 ASCII 字符列表(ASCII 值为十进制数值):

ASCII 值	字符
032	空格
033	!

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话: 025-83393092 传真: 025-83393091

URL: <http://www.jsca.com.cn>

036	\$
038	&
040	(
041)
045	-
046	.
047	/
048~057	0~9
058	:
065~090	A~Z
091	[
093]
094	^
095	_
096	`
097~122	a~z
123	{
125	}
126	~

7.1.5 证书策略对象标识符

证书策略由发证机构制定并对外广泛发布,同时向国际标准化组织申请标准的对象标识符(OID),从而保证与其它应用相兼容,对象标识符在通信服务中进行传递,作为该证书机构证书策略的标识,代表该认证机构提供证书服务的相关策略。另一方面,只有用户同意该证书策略,才可以从认证中心去申请和获得数字证书。

7.1.6 策略限制扩展项的用法

JSCA 未使用本扩展域。

7.1.7 策略限制符的语法和语义

JSCA 未使用本扩展域。

7.1.8 关键证书策略扩展项的处理规则

JSCA 未使用本扩展域。

7.2 CRL

7.2.1 版本号

JSCA 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。

JSCA 使用的 CRL 符合 X.500 标准

7.2.2 CRL 和 CRL 条目扩展项

- 颁发者

CN = JSCA_CA

OU = JSCA

O = 江苏省电子商务证书认证中心有限责任公司

L = 南京市

S = 江苏省

C = CN

- 生效日期

示例: 2005 年 9 月 20 日 10:18:45

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话: 025-83393092 传真: 025-83393091

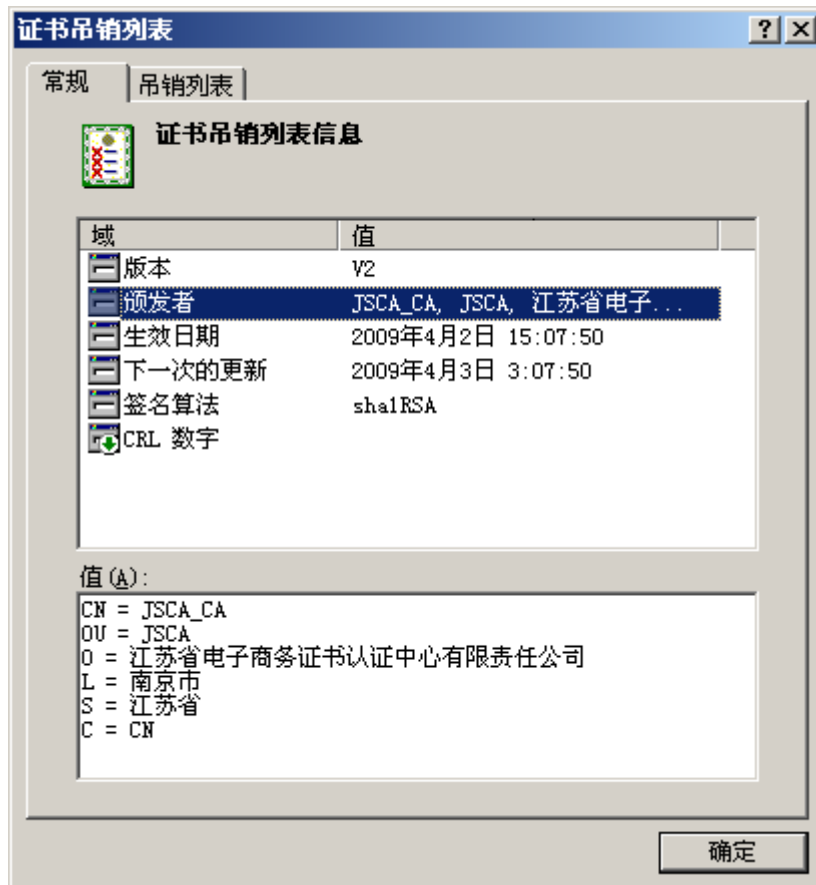
URL: <http://www.jsca.com.cn>

- 下一次的更新

示例：2005 年 10 月 20 日 10:18:45

- 签名算法

Sha1RSA



图表 1 证书吊销列表示例图

7.3 在线证书状态协议

暂未提供服务。

8 认证机构审计与评估

8.1 审计内容

对 JSCA 规范审计应包括：

JSCA 支持的证书认证操作规程是否完全与本认证业务声明表达一致，包括 JSCA 的技术、手续和员工的相关管理政策和业务声明。

JSCA 是否实施了相关技术、管理、相关政策和业务声明。

审计者或 JSCA 认为有必要审计的其他方面。

评估采用的规范和标准有 WebTrust 和 ISO27001 等。另外，还有对 JSCA 的财务评估和审计。

8.2 审计的频率与条件

根据情况而定，有年度评估、运营前评估、安全时间发生后的评估和随时进行的评估。

8.2.1 JSCA 的审计

由 JSCA 或法律主管部门指定审计者。审计者对 JSCA 进行审计。JSCA 本身也需要对 JSCA 的关联单位（包括 JSCA 授权的注册机构、注册分支机构、受理点等证书体系成员）所有的流程和操作进行审计，检验其是否符合本认证业务声明和相应的证书政策的规定，其频率可由 JSCA 决定或由法律制定的监管机构决定。

8.2.2 JSCA 对关联单位的审计

JSCA 对其关联单位实行定期审计（一般为一年）。审计人员由 JSCA 指派。

审计人员必须熟悉 JSCA 的规范和信任服务的相关知识，了解保证安全的基本知识
江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

识，按照 JSCA 的规范、协议、履行责任业务等情况独立、公正地对关联单位做出合格或不合格的结论。

JSCA 可以根据协议对下属的关联机构和单位进行安全审计，有权根据上级的审计结果和自己的审计结果，取消对下属单位的授权或重新授权。

JSCA 的关联单位，一年被审计的次数一般情况下为一次，特殊情况也不得超过二次。上级机构和单位，不得对下属单位和机构重复审计和重复收费。审计结果根据被审计单位的要求而决定是否公布。

8.3 审计者的身份与资质

8.3.1 JSCA 的内部审计

内部审计组织为 JSCA 运营安全管理小组，主要是审查实际运营操作是否与 JSCA CPS V1.2.2 中规定的一致。

8.4 不足信息的处理

如果在审计过程中发现执行规范有不足之处，报告公司领导，JSCA 将根据审计报告的内容准备一份解决方案，明确对此采取的相应行动。JSCA 将根据普遍认可的国际惯例或监管法律迅速解决问题。

8.5 审计结果

除非法律明确要求，JSCA 一般不公开审计结果。在必要的情况下，向 JSCA 关联单位（例如垫付商、注册机构、注册分支机构、受理点）通知审计结果的具体规定将在 JSCA 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 费用支付

JSCA 对证书持有者和垫付商收取服务费用。证书持有者和垫付商有义务根据 JSCA 的价目表支付给 JSCA 费用。

9.1.2 证书费用

证书认购的费用——根据江苏省物价局收费文件及 JSCA 的价目表；
证书更新的费用——根据江苏省物价局收费文件及 JSCA 的价目表；
密钥更新的费用——根据江苏省物价局收费文件及 JSCA 的价目表；
证书废止的费用——根据江苏省物价局收费文件及 JSCA 的价目表；
证书恢复的费用——根据江苏省物价局收费文件及 JSCA 的价目表；
其他与证书相关的费用——根据江苏省物价局收费文件及 JSCA 的价目表；

退款政策——JSCA 数字证书一旦发放，JSCA 不办理退证、退款手续。

9.2 财务责任

由于没有开设相应险种，目前没有保险。

9.3 业务信息保密

除非有法律要求，有关递交证书申请的用户信息将由 JSCA 保密并且在没有得到申请人授权的情况下不得泄漏。这不适用于证书中、或由 JSCA 得自公众的不涉及许可授权的用户信息。其他各参与方的商业计划、销售信息、贸易机密等

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

按照保密协议进行保密。

9.3.1 保密信息范围

保密信息有但不限于以下方面：

- 1、 在双方披露时标明为保密（或有类似标记）的；
- 2、 在保密情况下由双方披露的或知悉的；
- 3、 双方根据合理的商业判断应理解为机密数据和信息的；
- 4、 以其他书面或有形形式确认为保密信息的；
- 5、 或从上述信息中衍生出的信息。

对于 CA 来说有但不限于以下方面：

- 最终用户的私人签名密钥都是保密的，JSCA 和 RA 无权访问这些密钥。
- 保存在审计记录中的信息应由 JSCA 保密，除受法律要求，不可在公司外部发布。
- 年度审计结果也同样视为保密。
- 除非有法律要求，由 JSCA 和 RA 掌握的，除作为证书、CRL、认证策略被清楚发布之外的个人和公司的信息需要保密。

JSCA 不保存任何证书应用系统的交易信息。

9.3.2 不属于保密的信息

与证书有关的申请流程、申请需要的手续、申请操作指南等书中公布的信息是可以公开的。而且 JSCA 在处理申请业务时可利用这些信息，包括发布上述信息给第三方。

JSCA 在 JSCA 的目录服务器中公布证书的作废信息，供网上查询。

当 JSCA 在任何法律、法规或规章条款的要求下，或在法院的要求下必须披露本认证业务声明中具有保密性质的信息时，JSCA 可以按照法律、法规或规章条款以及法院的总协定的要求，向执法部门公布相关的保密信息。这种披露不视为违反了保密的要求和义务。

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

9.3.3 保护机密信息的责任

各方有保护自己和其他人员或单位的机密信息的并保证不泄露给第三方的责任。不将机密数据和信息（也不会促使或允许他人将机密数据和信息）用于协议项下活动目的之外的其他用途，包括但不限于将此保密信息的全部或部分进行仿照、反向工程、反汇编、逆向推导；在披露当时，如果已明确表示机密数据和信息不得复印、复制或储存于任何数据存储或检索系统，接受方不得复印、复制或储存机密数据和信息。

9.4 个人隐私保密

个人有保护自己和其他人员或单位的机密信息并保证不泄露给第三方的责任。

9.4.1 隐私保密方案

个人隐私信息保密方案遵守现行法律和政策。

9.4.2 作为隐私处理的信息

与证书持有者证书公钥配对的私有密钥是保密的，证书持有者应该认真保管，不能公布给他人。如果证书持有者擅自泄露私有密钥，则由此引起的后果由证书持有者自负。

JSCA 不保存用户的非公开信息。对于申请办理人的联系电话、电子邮件地址和通信地址等信息，非必要情况下不泄露。

9.4.3 不被视作隐私的信息

与证书持有者证书相关的信息，证书的相关信息是可以公开的，通过 JSCA 目录服务等方式向外公布。

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

证书被作废/暂停使用的信息披露。

当保密信息的所有者出于某种原因，要求 JSCA 公开或披露他所拥有的保密信息，JSCA 应满足其要求。

9.4.4 保护隐私的责任

在 JSCA 体系中的各方都有义务保护私密信息并避免泄露给第三方。

9.4.5 使用隐私信息的告知与同意

在授权下可以使用私密信息。

9.4.6 依法律或行政程序的信息披露

在政府管理和司法程序要求下有权使用私密信息。

9.4.7 其他信息披露情形

对于非故意的泄露机密信息的情况，根据国家法律处理。

9.5 知识产权

JSCA 享有并保留对证书以及 JSCA 提供的全部软件的知识产权，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，JSCA 有权决定关联机构采用什么软件系统，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。

按本认证业务声明的规定，所有与 JSCA 发行的证书和 JSCA 提供的软件相关的一切版权、商标和其他知识产权均属于 JSCA 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 JSCA 的同意后，可以使用江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

相关的文件和手册，并有责任和义务提出修改意见。

在没有 JSCA 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 JSCA 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

除非 JSCA 做出特别约定，若本认证业务声明的规定与其他 JSCA 制定的相关规定、指导方针相互抵触，用户必须接受本认证业务声明的约束。在 JSCA 与包括用户在内的其他方签订的仅约束签约双方的协议中，对协议中未约定的内容，视为双方均同意按本认证业务声明的规定执行；对协议中不同于本认证业务声明内容的约定，按双方协议中约定的内容执行。

责任范围：

JSCA 应承担的唯一和绝对的责任和义务是：

保证电子认证服务机构本身使用和发放的公钥算法在现有通常技术条件下不会被攻破；

保证 JSCA 的签名私有密钥在 JSCA 内部得到安全的存放和保护；

JSCA 建立和执行的安全机制符合国家政策的规定。

针对下述内容补充解释如下：

第一：除上述所规定的职责条款，JSCA、JSCA 的服务机构、JSCA 授权的发证机构、JSCA 的雇员不承担其它任何义务。必须指出，本认证业务声明的内容，没有任何信息可以暗示或解释成 JSCA 必须承担其它的义务或 JSCA 必须对其行为做出其它的承诺。

第二：在上述内容中所罗列情况及在发生不可抗力事件的情况下，江苏 CA 由于受到影响，可免除本节所述的责任和相应的证书策略规定的责任和义务。

第三：由于技术的进步与发展，为保证证书的安全性，JSCA 会要求证书持

有者及时更换证书以保证 JSCA 能更好地履行本节所述之责任。

9.6.2 注册机构的陈述与担保

注册机构必须遵守所有的登记程序和安全保障措施。这些程序和保障由 JSCA 决定,并在本认证业务声明或相应的注册机构协议中规定,以后 JSCA 可以根据情况修改有关内容,并及时公布。

注册机构必须遵守和符合本认证业务声明的条款,具体内容详见本文档第三章。

注册分支机构的职责:

同注册机构的职责。

受理点的职责:

同注册机构的职责。

9.6.3 用户的陈述与担保

所有的证书持有者必须严格遵守关于证书申请以及私有密钥的所有权和安全保存相关的程序:

证书持有者在证书申请表上填列的所有声明和信息必须是完整、精确、真实和正确的,可供 JSCA 或受理点检查和核实;

证书持有者必须严格遵守和服从认证业务声明规定的或者由 JSCA 推荐使用的安全措施;

证书持有者需熟悉本认证业务声明的条例和与证书相关的证书政策,还需遵守证书持有者证书使用方面的有关限制;

一旦发生任何可能导致安全性危机的情况,如证书持有者遗失私有密钥、遗忘或泄密以及其他情况,证书持有者应立刻通知 JSCA 或 JSCA 授权的发证机构,申请采取挂失、废除等处理措施。

申请人有以下义务:

1. 有义务为其在证书中的错误陈述承担责任,并应承担因其所提供的申请

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话: 025-83393092 传真: 025-83393091

URL: <http://www.jsca.com.cn>

信息侵犯他人权利而造成的后果的责任。

2. 有义务妥善保存自己的私钥，因私钥泄露造成的损失，由个人自己承担。

9.6.4 依赖方的陈述与担保

如果依赖方也是 JSCA 证书用户，依赖方本身也具有用户的责任和义务，对利用 JSCA 证书机制获得的信息负责，有验证对方身份的责任，包括验证证书使用者身份和数字签名，并用查询 JSCA 目录服务等方法来核实对方的证书有效性和资信。

9.6.5 其他参与者的陈述与担保

具有和依赖方相同的责任和义务。

9.7 担保免责

JSCA 不对由于不可抗力造成的操作失败或延迟承担任何损失、损坏或赔偿责任。

JSCA 在提供给证书持有者的“JSCA 数字证书用户责任书”中，都有事先告知证书持有者的免责条款的规定：JSCA 发放的各类型数字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。若证书持有者将其数字证书用于其他的用途，JSCA 不承担任何责任。

JSCA 在进行申请者身份认证或证书制作时，将充分遵守 JSCA 的安全操作流程。如果由于非 JSCA 的原因而造成的 JSCA 设备故障、线路中断，导致签发数字证书错误、延误、中断或者无法签发，JSCA 不负任何赔偿责任。

JSCA 在签发数字证书之前，证书申请者已同意遵守“JSCA 数字证书用户责任书”中的各项规定。用户责任书中明确规定 JSCA 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 JSCA 签发的数字证书，由此引起

的法律和经济责任由证书申请者全部承担，JSCA 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。JSCA 也不承担任何其他未经授权的人或组织以 JSCA 名义编撰、发表或散布不可信赖的信息所引起的法律责任。JSCA 仅提供电子沟通或交易中签名的“不可抵赖”的依据，但并不表明对此承担法律责任等方面的约定。

9.8 有限责任

JSCA 在与用户和依赖方签订的协议中，对于因用户或依赖方的原因造成的损害不具有赔偿义务。

9.9 理赔

9.9.1 JSCA 承担责任的限制

如 JSCA 违反了前文第 9.6 款条例规定的职责，JSCA 承担赔偿责任（法定或约定免责除外）的赔偿限制如下：

JSCA 所有的赔偿义务不得高于这种证书适用的赔偿责任上限。

赔偿责任上限为该种证书签发费、管理费和应用服务费总和的拾倍，最高不超过伍万元人民币。

证书签发费、管理费、应用服务费按江苏省物价局核准颁发的《收费许可证》中的规定执行。

JSCA 只有在 JSCA 证书有效期内承担损失损害赔偿。

9.9.2 注册机构承担责任的限制

注册机构的责任在注册机构和 JSCA 之间签订的注册机构协议中表明。

9.9.3 注册分支机构责任的限制

注册分支机构的责任在注册分支机构和 JSCA 之间签订的注册分支机构协议中表明。

9.9.4 受理点承担责任的限制

受理点的责任在受理点和 JSCA 之间签订的受理协议中表明。

9.10 有效期限和终止

JSCA 协议或文件中包含了对其全部、其一部分、其涉及应用的强制作用期和终止期。

9.10.1 有效期限

JSCA 的认证业务声明自发布之日起正式生效，文档中将详细注明版本号及发布日期，最新版本请访问 JSCA 网站，对具体个人不做另行通知，当新版本正式发布生效，旧版本将自动终止。

9.10.2 终止

文件全部、文件一部分、文件相关应用失效时作为终止期。

9.10.3 效力的终止与保留

在协议终止的情况下，有些条款依然是保留的，例如知识产权，需要继续履行。各方需要归还或保证销毁从其它方获得的机密信息。

9.11 对参与者的个别通告与沟通

JSCA 体系中各参与方之间都建立或具有个别沟通的渠道。

9.12 修订

对于 CPS 的由策略管理者认为是不重要的修改，CPS 可以不需要改版。反之，CPS 需要改版。

JSCA 有权在合适的时间修订、修改和改变本认证业务声明中任何术语、条件和条款，并自公布之日起三十日内向工业和信息化部备案。

JSCA 有权在自主数据库中设置和公布修改结果，或以其他方式（如修改版本的形式或在网站上）公布。

所有的修订、修改和改变在公布后立刻生效。

9.12.1 修订程序

- 1) 发现 CPS 中所列条款不能适应运营的实际需求,或者与现行法律相抵触;
- 2) 将现存问题反馈 CPS 编写小组;
- 3) 经过 CPS 编写小组讨论后,提出具体的修改意见;
- 4) 修改意见提交运营安全管理小组;
- 5) 运营安全管理小组审查修改意见,如果不通过则提出修改意见书反馈给 CPS 编写小组;
- 6) CPS 修改意见经运营安全管理小组审查通过,由 CPS 编写小组发布更新。

9.12.2 通知机制和期限

JSCA 和有关各方具有通知机制,定期或在需求或情况改变时不定期的征询各方意见。

9.12.3 必须修改业务规则的情形

当公司业务规则有重大改变时，需要修改 CPS。

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（约定为“南京仲裁委员会”），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

本认证业务声明在各方面服从中华人民共和国法律的管制和解释。

9.15 适用的法律的符合性

无论合同或其他法律条款的选择及无论是否在中国建立商业关系，JSCA 认证业务声明的执行、解释、翻译和有效性均适用中华人民共和国的法律。法律的选择是确保对所有用户有统一的程序和解释，而不管他们在何地居住以及在何处使用证书。

9.16 一般条款

9.16.1 完整协议

现行条款替代所有以前的和同时期的条款。

9.16.2 转让

通过某种方式限制一方的能力，如在协议中将一方的权利转让给另一方的规定或授权其某种义务。

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

9.16.3 分割性

在法律允许的范围内，在 JSCA 用户协议、依赖方协议和其他订货协议内出现可以同其他条款分割的条款时，协议中的可分割条款的无效不应该影响协议中其他条款的效力。

9.16.4 强制执行

合同一方或几方不履行合同条款的，其它方可以要求强制执行。

9.16.5 不可抗力

由于不可预见的原因和不可控的原因，视为不可抗力，会导致合同或协议的终止。JSCA 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。

9.17 其它条款

9.17.1 各种规范的冲突

若本认证业务声明的规定与其他规定、指导方针相互抵触，用户必须接受本认证业务声明的约束，除非本认证业务声明的规定在法律所禁止的范围内，或有关规定、指导方针明显优于本认证业务声明。

9.17.2 安全资料的财产权益

下列与安全相关的资料视为下列指定的当事人所拥有：

证书：证书的权利行使受 JSCA 的管理约束。本规范旨在保护用户的隐私，避免未经授权者公布其证书；

江苏省电子商务证书认证中心有限责任公司

南京市虎踞北路 10 号 电话：025-83393092 传真：025-83393091

URL: <http://www.jsca.com.cn>

65

认证业务声明：本认证业务声明的产权为 JSCA 所有；

甄别名：甄别名归命名实体所有（或他们的雇主和负责人所有）；

私有密钥：不论该密钥是以何种实体媒介存放或保护，私有密钥为合法使用或有权使用该密钥用户（或其雇主或委托人）所有；

公开密钥：不论该密钥以何种实体媒介存放或保护，公开密钥为用户（或其雇主或委托人）所有；

JSCA 的公开密钥：JSCA 作为自身的根节点的公开密钥，是 JSCA 的财产。这个公钥由 JSCA 授权分配，放在值得信任的硬体或软体上。

合同和协议中需要规定的其它条款。