安徽CA电子认证业务规则

(版本4.2)

（生效时间：2018年8月15日）

安徽省电子认证管理中心有限责任公司

安徽CA电子认证业务规则

安徽省电子认证管理中心有限责任公司版权所有

版权声明

对任何复制本文件的其他请求，请寄往以下地址：

安徽省电子认证管理中心有限责任公司

安徽省合肥市政务区白天鹅国际商务中心B座1803室

联系电话：0551-63497657 （技术部） 0551-63497653（办公室）

传 真：0551-63497653

本业务规则的最新版本请参见本公司网站http://www.aheca.cn，除法律法规另有要求，不再针对特定对象另行通知。

安徽CA CPS策略管理委员会负责本业务规则的解释。

安徽CA电子认证业务规则修订表

版本	发布日期	备注
1.0	2006年4月17日	根据《电子认证业务规则规范（试行）》编写
2.0	2006年9月1日	根据《电子认证业务规则规范（试行）》修订
3.0	2010年9月1日	根据《电子认证业务规则规范（试行）》、《中华人民共和国电子签名法》、《电子认证服务管理办法》修订
3.1	2011年10月25日	根据《电子认证服务管理办法》修订
4.0	2016年9月28日	根据《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》和工信部年检审查要求修订
4.1	2016年12月15日	更新了公司新的联系地址
4.2	2018年8月15日	根据新的业务模式进行修订

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.....3
1.3.1 电子认证服务机构.....3
1.3.2 注册机构（Registration Authority）.....3
1.3.3 证书持有者.....4
1.3.4 证书依赖方.....4
1.3.5 订户.....5
1.3.6 其他参与者.....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.....7
1.6 定义和缩写.....7
1.6.1 定义.....7
1.6.2 缩略语.....9
2 信息发布与信息管理.....11
2.1 认证信息的发布.....11
2.2 发布的时间或频率.....11
2.3 信息库访问控制.....11
3 身份识别与鉴别.....12
3.1 命名.....12
3.1.1 名称类型.....12
3.1.2 对名称意义化的要求.....12
3.1.3 订户的匿名或伪名.....12
3.1.4 理解不同名称形式的规则.....12
3.1.5 名称的唯一性.....12
3.1.6 商标的识别、鉴别和角色.....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 组织机构身份的鉴别.....13
3.2.3 个人身份的鉴别.....13
3.2.4 服务器证书订户身份的鉴别.....13

3.2.5 代码签名证书申请的身份鉴别 13
3.2.6 其他证书类型的身份鉴别 13
3.2.7 没有验证的订户信息 15
3.2.8 授权确认 15
3.2.9 互操作准则 15
3.3 密钥更新请求的标识与鉴别 15
3.3.1 常规密钥更新的标识与鉴别 15
3.3.2 吊销后密钥更新的标识与鉴别 16
3.4 吊销请求的标识与鉴别 16
4 证书生命周期操作要求 16
4.1 证书申请 16
4.1.1 证书申请实体 16
4.1.2 注册过程与责任 16
4.2 证书申请处理 17
4.2.1 执行识别与鉴别功能 17
4.2.2 证书申请批准和拒绝 17
4.2.3 处理证书申请的时间 17
4.3 证书签发 17
4.3.1 证书签发中注册机构和电子认证服务机构的行为 18
4.3.2 电子认证服务机构和注册机构对订户的通告 18
4.4 证书接受 18
4.4.1 构成接受证书的行为 18
4.4.2 电子认证服务机构对证书的发布 18
4.4.3 电子认证服务机构对其他实体的通告 18
4.5 密钥对和证书的使用 19
4.5.1 订户私钥和证书的使用 19
4.5.2 依赖方公钥和证书的使用 19
4.6 证书更新 20
4.6.1 证书更新的情形 20
4.6.2 请求证书更新的实体 20
4.6.3 证书更新请求的处理 20
4.6.4 颁发新证书时对订户的通告 20
4.6.5 构成接受更新证书的行为 20
4.6.6 电子认证服务机构对更新证书的发布 21
4.6.7 电子认证服务机构对其他实体的通告 21
4.7 证书密钥更新 21
4.7.1 证书密钥更新的情形 21
4.7.2 请求证书密钥更新的实体 21
4.7.3 证书密钥更新请求的处理 21
4.7.4 颁发新证书时对订户的通告 22
4.7.5 构成接受密钥更新证书的行为 22
4.7.6 电子认证服务机构对密钥更新证书的发布 22
4.7.7 电子认证服务机构对其他实体的通告 22
4.8 证书变更 22

4.8.1 证书变更的情形 22
4.8.2 请求证书变更的实体 23
4.8.3 证书变更请求的处理 23
4.8.4 颁发新证书时对订户的通告 23
4.8.5 构成接受变更证书的行为 23
4.8.6 电子认证服务机构对变更证书的发布 23
4.8.7 电子认证服务机构对其他实体的通告 23
4.9 证书吊销和挂起 24
4.9.1 证书吊销的情形 24
4.9.2 请求证书吊销的实体 24
4.9.3 吊销请求的流程 24
4.9.4 吊销请求宽限期 24
4.9.5 电子认证服务机构处理吊销请求的时限 24
4.9.6 依赖方检查证书吊销的要求 25
4.9.7 CRL 发布频率 25
4.9.8 CRL 发布的最大滞后时间 25
4.9.9 在线的吊销/状态查询的可用性 25
4.9.10 在线的吊销查询要求 25
4.9.11 吊销信息的其他发布形式 25
4.9.12 对密钥遭攻击的特别处理要求 25
4.9.13 证书挂起的情形 25
4.9.14 请求证书挂起的实体 26
4.9.15 挂起请求的流程 26
4.9.16 电子认证服务机构处理挂起请求的时限 26
4.9.17 挂起的期限限制 26
4.10 证书状态服务 26
4.10.1 操作特征 26
4.10.2 服务可用性 26
4.10.3 可选特征 27
4.11 订购结束 27
4.12 密钥生成、备份与恢复 27
4.12.1 密钥生成、备份与恢复的策略与行为 27
4.12.2 会话密钥封装和恢复策略与行为 28
5 认证机构设施、管理和操作控制 28
5.1 物理控制 28
5.1.1 场地位置与建筑 28
5.1.2 物理访问 28
5.1.3 电力与空调 28
5.1.4 水患防治 28
5.1.5 火灾防护 29
5.1.6 介质存储 29
5.1.7 废物处理 29
5.1.8 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.....31
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 独立和约人的要求.....32
5.3.8 提供给员工的文档.....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.....33
5.4.3 审计日志的保存期限.....33
5.4.4 审计日志的保护.....33
5.4.5 审计日志备份程序.....33
5.4.6 审计收集系统.....33
5.4.7 对导致事件实体的通告.....33
5.4.8 脆弱性评估.....33
5.5 记录归档.....34
5.5.1 归档记录的类型.....34
5.5.2 归档记录的保存期限.....34
5.5.3 归档文件的保护.....34
5.5.4 归档文件的备份程序.....34
5.5.5 记录的时间戳要求.....35
5.5.6 归档收集系统.....35
5.5.7 获得和检验归档信息的程序.....35
5.6 电子认证服务机构密钥更替.....35
5.7 事故与灾难恢复.....36
5.7.1 事故和损害处理流程.....36
5.7.2 计算资源、软件和/或数据的损坏.....36
5.7.3 实体私钥损害处理程序.....36
5.7.4 灾难后的业务连续性能力.....36
5.8 电子认证服务机构或注册机构的终止.....37
6 认证系统技术安全控制.....37
6.1 密钥对的生成和安装.....37
6.1.1 密钥对的生成.....37
6.1.2 私钥传送给订户.....37
6.1.3 公钥传送给证书签发机构.....37
6.1.4 电子认证服务机构公钥传送给依赖方.....37
6.1.5 密钥的长度.....37

6.1.6 公钥参数的生成和质量检查 38
6.1.7 密钥使用目的 38
6.2 私钥保护和密码模块工程控制 38
6.2.1 密码模块标准和控制 38
6.2.2 私钥多人控制（m 选 n） 38
6.2.3 私钥托管 39
6.2.4 私钥备份 39
6.2.5 私钥归档 39
6.2.6 私钥导入、导出密码模块 39
6.2.7 私钥在密码模块的存储 39
6.2.8 激活私钥的方法 40
6.2.9 解除私钥激活状态的方法 40
6.2.10 销毁私钥的方法 40
6.2.11 密码模块的评估 40
6.3 密钥对管理的其它方面 41
6.3.1 公钥归档 41
6.3.2 证书操作期和密钥对使用期限 41
6.4 计算机安全控制 41
6.4.1 特别的计算机安全技术要求 41
6.4.2 计算机安全评估 41
6.5 生命周期技术控制 41
6.5.1 系统开发控制 41
6.5.2 安全管理控制 42
6.5.3 生命期的安全控制 42
6.6 网络的安全控制 42
6.7 时间戳 43
7 证书、证书吊销列表和在线证书状态协议 43
7.1 证书 43
7.1.1 版本号 43
7.1.2 证书扩展项 43
7.1.3 证书标准项 43
7.1.4 算法对象标识符 44
7.1.5 名称形式 44
7.1.6 名称限制 44
7.1.7 证书策略对象标识符 44
7.1.8 策略限制扩展项的用法 45
7.1.9 策略限定符的语法和语义 45
7.1.10 关键证书策略扩展项的处理规则 45
7.2 CRL 45
7.2.1 版本号 45
7.2.2 CRL 和 CRL 条目扩展项 45
7.3 在线证书状态协议 46
7.3.1 版本号 46
7.3.2 OCSP 扩展项 46

8 认证机构审计和其它评估 46
8.1 评估的频率或情形 46
8.2 评估者的资质 47
8.3 评估者与被评估者的关系 47
8.4 评估内容 47
8.5 对问题与不足采取的措施 47
8.6 评估结果的传达与发布 48
9 法律责任和其他业务条款 48
9.1 费用 48
9.1.1 证书签发和更新费用 48
9.1.2 证书查询费用 48
9.1.3 证书吊销或状态信息的查询费用 48
9.1.4 其它服务费用 48
9.1.5 退款策略 48
9.2 财务责任 49
9.3 业务信息保密 49
9.3.1 保密信息范围 49
9.3.2 不属于保密的信息 50
9.3.3 保护机密信息的责任 50
9.4 个人信息私密性 50
9.4.1 隐私保密方案 50
9.4.2 作为隐私处理的信息 51
9.4.3 不视为隐私的信息 51
9.4.4 保护隐私的责任 51
9.4.5 使用隐私的告知与同意 51
9.4.6 其它信息披露情形 51
9.5 知识产权 52
9.6 陈述与担保 52
9.6.1 安徽 CA 的陈述与担保 52
9.6.2 RA 的陈述与担保 55
9.6.3 受理点的陈述与担保 55
9.6.4 证书持有者的陈述与担保 56
9.6.5 证书依赖方的陈述与担保 56
9.6.6 其他参与者的陈述与担保 57
9.7 有限责任与免责条款 57
9.7.1 特定责任的排除 57
9.7.2 免责条款 57
9.8 赔偿 59
9.8.1 理赔 59
9.8.2 索赔 59
9.9 CPS 的有效期与终止 60
9.10 CPS 的修订 60
9.11 争议解决 60
9.12 管辖法律 60

9.13 与适用法律的符合性..... 61
9.14 一般条款.....61
9.14.1 完整协议.....61
9.14. 2 分割性.....61
9.14. 3 强制执行.....61
9.14. 4 不可抗力.....61
9.15 各种规范的冲突.....61
9.16 补充说明.....62

1 概括性描述

1.1 概述

安徽省电子认证管理中心有限责任公司（简称安徽CA，英文简称AHCA）是经国家相关部门批准成立的专业化的第三方认证机构，建有独立密钥管理中心。安徽CA作为公正权威的第三方安全认证机构，是信息安全的基础设施，以密码技术为核心技术，其签发的电子证书是电子政务、电子商务等业务的信息交换中确认身份、控制权限，保证信息源真实性、完整性和信息发送不可抵赖性的重要手段。对网络防泄密、抗侵入、拒黑客、识真伪、保安全有着不可替代的重要作用。安徽CA签发的电子证书，具有权威性和公正性，能为公众用户提供第三方国家商密保护的信息安全服务。

安徽CA的电子认证业务规则（CPS）阐明了安徽CA作为一个证书认证机构如何根据安徽CA的证书策略开展其业务，包括批准、管理、吊销和更新证书业务方式和过程，相应的服务、法律和技术上的措施和保障。

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）、《中华人民共和国电子签名法》（2005年4 月1 日起施行）、中华人民共和国信息产业部发布的《电子认证服务管理办法》（2005 年4 月1 日起施行）以及中华人民共和国信息产业部电子认证服务管理办公室编写的《电子认证业务规则规范（试行）》。安徽省电子认证管理中心有限责任公司依据《中华人民共和国电子签名法》、《合同法》等相关的国家法律法规，根据自身的实际运营情况于2006年8月进行了修订，并于2006年9月1日开始正式执行。

安徽CA负责其下属的电子证书注册机构（RA）、电子证书受理点的建设和运行管理。安徽CA的主要业务内容包括：

（一） 制作、签发、管理电子证书；

（二） 对签发的电子证书的真实性进行确认；

（三） 提供电子文件认证服务；

（四） 提供电子证书目录查询服务；

（五） 其他经主管部门核准办理的业务。

利用安徽CA签发的电子证书以及相关PKI 技术可以实现以下功能：

（一） 能够确认数据电文签署人的身份；

（二） 能够保证数据电文在传递、接收和储存过程中的完整性；

（三） 能够避免系统被侵入或者人为破坏以及数据电文被篡改；

（四） 能够保证网络信息的安全加密、解密。（描述统一，规范）

安徽CA电子认证业务规则（CPS，Certification Practice Statement）是安徽CA对所提供的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）所遵循的规范的详细描述和声明，包括责任范围、作业操作规范和信息安全保障措施等内容，是证书管理、证书服务、证书应用、证书分类、证书授权、证书责任等政策规则的集合，主要由以下几部分组成：

（一）概括性描述

（二）信息发布与信息管理

（三）身份标识与鉴别

（四）证书生命周期操作要求

（五）认证机构设施、管理和操作控制

（六）认证系统技术安全控制

（七）证书、证书吊销列表和在线证书状态协议

（八）认证机构审计和其他评估

（九）法律责任和其他业务条款

安徽CA认证体系内的实体以及安徽CA电子证书持有者，必须完整地理解和执行安徽CA电子认证业务规则所规定的条款，承担相应的责任和义务。

1.2 文档名称与标识

本文档名称：《安徽CA电子认证业务规则》。

本电子认证业务规则为安徽CA发布的第四个版本。

本电子认证业务规则在安徽CA的网站上予以发布：http://www.aheca.cn。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

安徽CA是所有安徽CA下层机构和实体的根。安徽CA的实际运作管理单位是安徽省电子认证管理中心有限责任公司。

安徽CA制定安徽CA管理文档，各种审计记录和各类表单所形成的日志，其中包括安徽CA对外运营策略和规范的管理。并且同时提供每周7天，每天24小时管理计划和维护计划。安徽CA依法向证书申请者颁发证书、撤销证书、发布证书注销列表等对证书操作的一系列流程，并为安徽CA制定出具体政策、管理制度、运作规范和相关的规则。安徽CA根据国家相应的法律制定安徽CA法律责任书，并有权让证书用户遵守安徽CA的规定。安徽CA制定财务责任书，并有权让证书用户遵守安徽CA的规定。安徽CA认证系统采用国际领先的PKI 技术，采用双层结构，最高层也就是第一层CA叫做根CA，由国家根CA提供，安徽CA称为二级CA用于签发证书。安徽CA由证书认证机构（CA）和证书注册审批机构（RA）两大部分组成。

1.3.2 注册机构（Registration Authority）

电子证书注册机构（Registration Authority），简称RA，是安徽CA授权委托的下属机构，是安徽CA数字认证体系的一个组成部分，在安徽CA的统一领导和集中管理下开展业务活动。

安徽CA的RA系统分为本地RA和外部RA。

本地RA：指RA服务器设立在安徽CA的RA 系统，现分为两种：一种为安徽CA直属RA，归安徽CA所有，由安徽CA使用，为证书总量相对较小（在5000 以下）的企业提供证书申请审批、证书信息录入以及证书发放并进行部分管理服务，适合于不建立RA 系统、没有RA 操作人员的企业和组织使用。另一种为托管RA，归托管RA 的企业或组织所有，由托管RA 的企业或组织使用，为证书总量相对较小（在5000 以下）或证书审核严格或证书管理复杂的的企业和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，适合于需要对RA 系统功能进行客户化定制和需要自主管理RA 系统的企业和组织使用。证书总量在5000以上的我们建议建立企业自由RA机构，以便于有效的管理和服务。

外部RA：指RA服务器设立在企业或组织中的RA系统，归企业或组织所有，由企业或组织使用，为证书总量较大或证书审核严格或证书管理复杂的企业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，采用安全方式与安徽CA连接。外部RA现分两种：一种为直连RA，RA服务器通过Internet或者专线按照CA的接口与安徽CA系统直接相连，进行数据和指令的传输。一种为前置机RA,RA系统和安徽CA的前置机系统(简称FEP)相连，这种方式下，对CA系统的安全可靠性控制和集成化程度更高，隐藏了接口的复杂性，为用户提供更为简单易用的RA开发接口。处理方式有两种：批处理方式和联机实时处理方式。

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安徽CA的CA服务器交换数据。对于直属RA的情况，RA服务器和LRA均在安徽CA；对于托管RA的情况，RA服务器在安徽CA但由托管方操作，LRA设在托管方；对于外部RA的情况，RA服务器在组织机构的总部，在需要应用证书的分支机构设置LRA。

1.3.3 证书持有者

证书持有者，也称为证书用户，指持有安徽CA颁发的各类证书且持有与列示于证书中的公钥相对应的私钥的人、物对象或单位组织，包括个人、企业、团体、提供网上服务或享受网上服务的实体和应用服务器等。

1.3.4 证书依赖方

证书依赖方是指在安徽CA证书服务体系之内作为依赖于电子证书真实性的实体，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。在安徽CA体系中，是信任安徽CA证书，可以对使用安徽CA证书机制进行的数字签名进行验证，使用其他安徽CA证书用户的公钥加密信息的实体。

1.3.5 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。指证书和证书相关服务的使用者，目前安徽CA的电子证书在电子商务和电子政务领域有广泛的应用。

1.3.6 其他参与者

指在安徽CA证书应用体系和服务体系中除上述的电子认证机构、电子证书注册机构、电子证书受理点、证书持有者、证书依赖方、证书申请者之外的其他实体。

1.4 证书应用

1.4.1 适合的证书应用

安徽CA拥有下表所属的电子证书类型。除安徽CA电子认证业务规则或证书自身禁止，使用安徽CA所提供的任何证书应由每个证书申请者自由选择。

安徽CA电子证书种类及应用范围

证书种类	应用范围
个人安全电子邮件证书	安全电子邮件传送或向需要客户验证的Web服务器表明身份
个人身份证书	个人在网上活动中表明身份
企业或机构安全电子邮件证书	安全电子邮件传送或向需要客户验证的Web服务器表明身份
企业或机构身份证书	在企业的电子商务活动中表明企业身份
服务器证书	用于表明服务器身份，主要用于网站交易服务器

1.4.2 限制的证书应用

对于使用未经安徽CA认可的证书应用软件来保护安全的系统，不适用安徽CA证书。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。

1.5 策略管理

策略权威为安全经理，负责收集安全策略委员会其他成员的建议和意见，使其达成一致意见，同时负责开发、维护认证策略文件（CP）。安全策略委员会成员负责对该CPS进行审核，以确保CPS文件与CP文件保持一致。通常根据需要安全策略委员会每年举行至少1次会议。安全策略委员会的成员可由来自于综合部、财务部、系统保障部、技术开发部以及技术支持部等部门的代表组成。

1.5.1 策略文档管理机构

本电子认证业务规则的制订、更新、发布等事宜，其管理机构为安徽CACPS编写和维护组，安徽CA完全拥有本电子认证业务规则的版权。

1.5.2 联系人

联系人：安徽CA办公室 徐常斌

地址：安徽省合肥市政务区白天鹅国际商务中心B座1803室

电话：0551-63497653　63497657

传真：0551-63497653

电子邮址： ahca@aheca.cn

1.5.3 决定 CPS 符合策略的机构

安徽省电子认证管理中心有限责任公司安全策略委员会拥有对安徽CA电子认证业务规则的决策权和审批权。

1.5.4 CPS 批准程序

CPS 批准主要分为计划、编写、审议和发布四个阶段：

（1） 计划：安徽CACPS 编写维护组根据相关法律政策和运营策略提出CPS 编写（修订）计划。

（2） 编写：CPS 编写维护组，完成具体条款编写工作。

（3） 审议：编写（修订）后的CPS 递交安徽CA安全策略委员会，并由安全策略委员会进行审议。

（4） 发布：安徽CA安全策略委员会审议通过后，在征询安徽CA律师的意见后，通过安徽CA网站或其他形式正式对外发布。

1.6 定义和缩写

1.6.1 定义

（1）公钥基础设施（PKI）：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，提供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。

（2）认证中心（CA）：受用户信任的，负责创建和签发电子证书的权威机构。CA 是认证中心的英文Certification Authority 的缩写。CA 中心，又称为电子证书认证中心。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电子证书，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。

（3）注册机构（RA）：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 和外部RA 两种。

（4）本地RA：指RA 服务器设立在安徽CA的RA 系统，分为直属RA 和托管RA 两种。

（5）直属RA：指归安徽CA所有，由安徽CA使用，为证书总量相对较小（在5000以下）的企业提供证书申请审批、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。

（6）托管RA：指归托管RA 的企业或组织所有，由托管RA 的企业或组织使用，为证书总量相对较小（在5000 以下）或证书审核严格或证书管理复杂的的企业和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。

（7）外部RA：指RA 服务器设立在企业或组织中的RA 系统，归企业或组织所有，由企业或组织使用，为证书总量较大（在5000 以上）或证书审核严格或证书管理复杂的企业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。分为直连RA 和前置机RA 两种安全方式与安徽CA连接。

（8）直连RA：指采用RA 服务器通过Internet 或者专线按照CA 的接口与安徽CA系统直接相连，进行数据和指令的传输的方式RA 系统。

（9）前置机RA：指RA 系统和安徽CA的前置机系统(简称FEP)相连，由前置机系统进行处理后再通过前置机系统和CA 服务器进行数据和指令的传输的方式RA 系统。

（10）电子证书（Digital Certificate）：经CA 数字签名的包含电子证书使用者身份公开信息和公开密钥的电子文件。由于Internet 网上的电子商务系统技术使某些敏感或有价值的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。电子证书提供了一种在Internet 上验证身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。

（11）证书吊销列表（CRL）：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某些电子证书不再有效。

（12）在线证书状态协议（OCSP）：IETF 颁布的用于检查电子证书在某一交易时间是否有效的标准。

（13）证书策略（CP，Certificate Policy）：一套命名的规则集，用以指

明证书对一个特定团体和（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企业到企业（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。

（14）电子认证业务规则（CPS）：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的描述。包括CA 整体运行规范和证书的颁发、管理、吊销和密钥以及证书更新的操作规范等事务。

（15）订户(Subscriber)：被颁发给一个证书的证书主体。

（16）依赖方(Relying party)：证书的接收者，他依赖于该证书和（或）该证书所验证的数字签名。在本标准中，术语“证书使用者”与“依赖方”可互换使用。

（17）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、编码等数据。

（18）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。

（19）唯一甄别名(DN,Distinguished Name)：在电子证书的主体名称域中，用来唯一标识用户的X.509 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。

1.6.2 缩略语

安徽CA AnHui Certification Authority 安徽省电子认证管理中心

ARL Authority Revocation List 授权注销列表

ACL Access Control List 访问控制列表

CA Certification Authority 认证权威

CP Certificate Policy 认证策略

CPS Certification Practice Statement 认证业务说明

CRL Certificate Revocation List 证书注销列表

DAP DirectoryAccess Protocol 目录访问协议

DES Data Encryption Standard 数据加密标准

DN Distinguished Name 甄别名称

DNS Domain Name Server 域名服务器

DSA/DSS Digital Signature Algorithm/ Digital SignatureStandard 数字签名算法/数字签名标准

FIPS Federal Information Processing Standard 国家信息处理标准

GSS-API Generic Security Service ApplicationProgramming Interface 通用安全服务应用程序接口

HTTP Hypertext Transfer Protocol 超文本传输协议

I&A Identification and Authentication 鉴别与认证

IETF Internet Engineering Task Force 因特网工程任务组

ISO Information Security Officer 信息安全官员

ITU International Telecommunications Union 国际电信联盟

LDAP Lightweight DirectoryAccess Protocol 轻量目录访问协议

RA Registration Authority 注册权威

OA Operational Authority 操作权威

PIN Personal Identification Number 个人识别码

PKI Public Key Infrastructure 公钥基础设施

PKIX Public Key Infrastructure X.509 公钥基础设施X.509

PMA Policy Management Authority 政策管理权威

PUB Publication 出版

RFC (IETF)Request For Comments 意见要求

RSA Rivest-Shamir-Adleman RSA 算法

S/MIME Secure/Multipurpose Internet Mail Extensions 安全/多用途因特网邮件扩展

SHA-1 Secure Hash Algorithm 安全散列算法

S-HTTP Secure Hypertext Transfer Protocol 安全Http 协议

SMTP Simple Mail Transfer Protocol 简单邮件传输协议

SPKM Simple Public-Key GSS-API Mechanism 简单公钥接口机制

SSL Secure Sockets Layer 安全套接字层

TRA Threat and Risk Assessment 威胁和风险评估

URI Uniform Resource Identifier 统一资源标识符

URL Uniform Resource Locator 统一资源定位符

2 信息发布与信息管理

2.1 认证信息的发布

根据X.509 标准，安徽CA 在对外的目录服务器公布证书的相关信息，并以定期和定时的方式公布证书吊销列表CRL，CPS在安徽CA的网站上发布。

2.2 发布的时间或频率

★ 安徽CA签发的证书在最终用户收到证书之后立即发布。

★ 安徽CA的CRL可以实时发布和定期发布。

★ CPS在版本更新后立即在网站(http://www.aheca.cn)上更新发布。

2.3 信息库访问控制

★ 在安徽CA,只有经过严格授权的CA管理员可以访问CA数据库中的数据；

★ 在安徽CA,只有经过严格授权的RA管理员可以访问存储在RA服务器数据库中的数据；

★ 用户可以访问安徽CA目录服务器中的数据，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

证书从应用角度分为系统证书和用户证书，命名由用户应用决定。

3.1.1 名称类型

安徽CA证书体系中采用X.509定义的甄别名称（DN）标准来唯一标识一张证书使用者的身份信息。

根据证书对应实体的类型不同，安徽CA签发的证书的实体名字可以是人员姓名、组织机构名称、部门名称、域名等，命名符合X.509甄别规定。

3.1.2 对名称意义化的要求

根据证书应用范围决定证书名称，以方便证书应用系统使用者。

3.1.3 订户的匿名或伪名

用户申请电子证书时需带上有效的证件（个人：身份证、军官证、学生证等；企业：营业执照、代码证、税务登记证等）到业务受理处进行注册，通过验证后，才有申请电子证书的权利。根据安徽CA的电子认证业务规则，安徽CA不接受匿名及使用伪名的客户所提交的电子证书申请请求，因而匿名及使用伪名的客户将无法获得安徽CA所签发的电子证书。

3.1.4 理解不同名称形式的规则

证书系统可以通过X.509 V3 证书内容的扩展属性部分，使证书带有不同的名称形式反应不同的等级权限，规则的设定根据证书的管理策略来制定。

3.1.5 名称的唯一性

在安徽CA所签发的电子证书中，用DN （Distinguished Name）项来唯一标识用户的证书名称。用户申请证书时，证书系统会自动对其唯一性进行审核。如

果不能通过唯一性审核，证书系统将拒绝签发证书。

3.1.6 商标的识别、鉴别和角色

企业用户在证书申请前需要提交企业营业执照及组织机构代码证的复印件并出示原件，对它的验证就是对企业资信的验证，同时用企业申请到的电子证书进行的操作视作企业行为。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

在安徽CA的体系中，用户签名私钥（private key）在用户端生成，用户的私钥保存在安全介质中发放给用户，用户可以通过专用工具对私钥进行使用（如数字签名）。合法的用户是其私钥的唯一持有者。因此，安徽CA要求用户必须妥善保管自己的私钥。

3.2.2 组织机构身份的鉴别

组织机构用户向RA 或LRA 出示经办人的身份证件和EMAIL 地址、企业合法证件（工商营业执照、全国组织机构代码证书）等来证明他们的身份。另外还要求企业给经办人办理证书申请事宜的授权书以及经办人身份证件的复印件。

3.2.3 个人身份的鉴别

个人用户通过向RA或LRA出示其身份证（护照和军官证）、学生证、工作证等合法可信的个人证明来证明他们的身份。

3.2.4 服务器证书订户身份的鉴别

订户如需要申请普通 SSL 服务器证书，只能向 AHCA 提交申请，AHCA 可以受理机构订户、个人订户的申请。普通 SSL 服务器证书可以包含多域名、通配符证书。订户申请SSL 服务器证书时，应提交如下材料：

1、证书申请表

2、至少一种机构身份证件（个人订户不适用）

3、申请人的个人身份证件

4、机构授予申请人的授权证明（个人订户不适用）

5、拥有公网IP 的证明（域名型的不需要）

6、证书申请CSR 文件

AHCA 除对申请者的身份、地址信息、国家信息等进行鉴别外，还要对域名或者外网IP及CSR 合规性进行鉴别。其鉴别流程方法如下。

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

对于公网 IP 的鉴别，订户可提供 ISP 商分配 IP 的纸质盖章证明材料或者ISP 的邮件证明材料。

如果申请通配符域名证书，AHCA 将鉴别其拥有的二级域名。对于多域名证书,AHCA 将对所有列举的域名进行鉴别。对于 CSR 文件的鉴别主要包含,CSR 中的信息是否与申请表中的申请信息一致,是否符合相关规范,比如 DN 的顺序等,并验证其是否拥有私钥。

3.2.5 代码签名证书申请的身份鉴别

订户如需要申请代码签名证书，只能向 AHCA 提交申请，AHCA 受理个人用户和机构订户申请该类证书。代码签名证书应提交如下材料：

1、证书申请表

2、至少一种机构身份证件（申请企业/组织证书）（个人不需要）

3、申请人的个人身份证件

4、机构授予申请人的授权证明（申请企业/组织证书）

AHCA 对申请者的身份、地址信息、国家信息等进行鉴别，其鉴别方法如下：如果验证对象为企业，需验证用户企业的合法性、企业的实体存在和商业行为的存在（此企业有正常的商业行为），还要认证申请人是否有资格代表企业， 不对其代码进行鉴别。

3.2.6 其他证书类型的身份鉴别

针对设备证书、VPN 证书等，需要鉴别申请者的身份、地址、国家，不对其设备进行验证。

针对安全邮件证书，AHCA 将只受理可在域名注册信息查询(whois)功能里查询到的域名邮件申请，并通过适当的途径鉴别该邮件地址是否合法、有效， 同时鉴别申请人的身份信息、地址、国家等信息。

针对预植证书、场景证书以及云证通证书的鉴别参照个人身份、企业身份方法进行鉴别，也可以采取适当的自动鉴别方式。

3.2.7 没有验证的订户信息

审核由RA 实现，根据认证中心制定的策略审核用户，没有通过验证则拒绝发放证书。证书无法继续获得信任的时候，不论任何原因都将证书撤销。

3.2.8 授权确认

对于不同的证书申请人，根据使用范围授予不同的权限。

系统证书指安徽CA系统内部证书，包括首席官员证书、管理员证书；

用户证书可以将其分为个人用户证书、单位用户证书、服务器证书、部门证书、电子邮件证书等。

3.2.9 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

在常规密钥更新中，通过订户使用当前有效私钥对包含新公钥的密钥更新请求进行签名，安徽CA使用订户原有公钥验证确认签名来进行订户身份标识和鉴

别。

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安徽CA证书服务。详见3.2.2 组织身份的鉴别和3.2.3个人身份的鉴别。

3.4 吊销请求的标识与鉴别

订户本人吊销时的身份标识和鉴别使用原始身份验证相同的流程，详见3.2.2组织身份的鉴别和3.2.3个人身份的鉴别。

如果是因为订户没有履行本CPS所规定的义务，由注册机构申请吊销订户的证书时，不需要对订户进行标识和鉴别。

满足“证书吊销条件”的情况时，安徽CA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安徽CA的RA系统来进行吊销操作。

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

用户证书的申请审核由RA 实现，RA 根据认证中心制定的策略审核用户，批准申请或拒绝发放证书。

注册机构负责收集申请人的身份识别文件并采取合理的措施确保颁发证书的有效性和真实性。

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。

★ 用户要按照安徽CA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. 用户递交证书申请材料到安徽CA；

2. 处理证书申请材料时，由双人控制，安徽CA注册人员首先对证书申请材料进行审核，审核人员将对证书申请材料进行第二次审核。

证书申请材料包括证书申请表和以下材料：

企业用户：参照 3.2.2 节的规定。

个人用户：参照 3.2.3 节的规定。

安徽CA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者拒绝发放证书。

4.2.3 处理证书申请的时间

安徽CA在收到证书申请材料后应在24小时内予以处理。

4.3 证书签发

证书的签发过程是：安徽CA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，安徽CA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订户的通告

为用户制证后将用户证书直接或通过有效安全的途径发放给用户，并将用户的公钥证书发布到主从LDAP上，以供用户在线查询证书。同时，可以通过在线方式实现对证书撤销列表（CRL）的查询。

4.4 证书接受

4.4.1 构成接受证书的行为

在安徽CA 电子证书签发完成后，申请者至安徽CA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。证书申请者接受电子证书后，应妥善保存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

安徽CA在签发完证书后，将把证书及公钥信息发布到安徽CA系统的目录服务器中，通过网站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

安徽CA系统提供对证书在线状态查询协议的支持，证书成功下载后，证书是否可以信任，用户可以通过标准的证书状态查询接口来获取证书有效性的检查结果。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

用户的密钥对有两对，一对用于签名和验证签名，另一对用于信息的加密和解密，其中用于加密、解密的密钥对由密钥管理中心产生，在加密机中使用主密钥加密后，将加密的用户密钥对读出放在数据库中保存。用于签名和验证的密钥对由客户端工具产生并管理。对于签名证书，其私钥可以用于对信息的签名。在可能的情况下，签名证书及其信任链上证书（根本证书除外）应同被签名信息一起提交给依赖方。证书持有人使用私钥对信息签名时，应该知晓并确认被签名的内容。对于具有身份鉴别用途的证书，其私钥可以用于对鉴别方提交的信息签名；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。证书持有人应妥善保管其证书私钥。用户需要妥善保管自己的私钥和证书，不将其用于不适合的证书用途，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

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。

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，须先经过适当的途径获得接受方的加密证书然后使用加密证书上的公钥对信息加密，依赖方应该连同加密证书和加密信息一起发送给接受方。

4.6 证书更新

4.6.1 证书更新的情形

有三种情形需要更新密钥对：

1．加密公钥或签名私钥的使用期限已经过期。（包括快要过期）

2．加密公钥或签名私钥已经或怀疑泄密，该密钥对作废，而且相对应的证书的序列号由管理员放入证书注销列表（CRL）。

3．用户的甄别名称变更。

4.6.2 请求证书更新的实体

由安徽CA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、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，以及其他凡是安徽CA各类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

安徽CA处理证书更新时首先用户提出证书更新申请后，安徽CA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；审核通过后，由管理员在证书业务处理终端对用户的证书进行更新。

身份鉴别方式和处理参照3.2.2 组织机构身份的鉴别和3.2.3 个人身份的鉴别要求相同。

4.6.4 颁发新证书时对订户的通告

证书制作后将用户证书直接或通过有效安全的途径发放给用户，并将用户的公钥证书发布到主从LDAP上，以供用户在线查询证书。同时，可以通过在线方式实现对证书撤销列表（CRL）的查询。

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，安徽CA的 RA 执行证书更新操作；

2. 安徽CA 根据 X.509 标准用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

证书查询和CRL 查询功能主要采用LDAP协议。

CA 系统签发证书后，将用户的证书发布到系统的主目录服务器中，然后利用主目录服务器的自动映射功能，将用户的证书发布到从目录服务器中，以供用户在线查询证书。

CA系统在目录服务器系统中发布CRL，因此用户可以通过在线方式实现对CRL的查询。

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，其他用户可以在安徽CA网站上的在线业务下面查验到。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

出现下列情形之一时证书密钥需要更新：

★ 用户忘记了使用密码。

★ 证书无法继续获得信任。

★ 证书和密钥对到期。

★ 证书丢失或者无法正常使用。

4.7.2 请求证书密钥更新的实体

证书更新申请者为安徽CA的合法证书用户。

4.7.3 证书密钥更新请求的处理

安徽CA 证书用户向安徽CA的RA递交证书密钥更新请求，由RA审核用户的申

请材料。 审核通过后，安徽CA的RA更新证书密钥并通知用户。

身份鉴别方式和处理参照3.2.2 组织机构身份的鉴别和3.2.3 个人身份的鉴别要求相同。

4.7.4 颁发新证书时对订户的通告

证书制作后将用户证书直接或通过有效安全的途径发放给用户，并将用户的公钥证书发布到主从LDAP上，以供用户在线查询证书。同时，可以通过在线方式实现对证书撤销列表（CRL）的查询。

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. 安徽CA RA执行证书密钥更新行为
2. 安徽CA 根据X.509标准用用户的公开信息组成新的证书信息。

4.7.6 电子认证服务机构对密钥更新证书的发布

安徽CA在签发更新证书后，就将新证书发布到数据库和目录服务器中，通过安徽CA的网站中在线证书状态查询的服务提供。

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，其它用户可以在安徽CA网站上的在线证书状态查询中查到。

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，安徽CA证书用户可以向安徽CA申请证书变更 。

4.8.2 请求证书变更的实体

合法的安徽CA的证书用户。

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安徽CA提出证书更新请求。
2. 安徽CA对有效证件进行审核。
3. 审核通过后，由RA管理员进行更新处理。

身份鉴别方式和处理参照3.2.2 组织机构身份的鉴别和3.2.3 个人身份的鉴别要求相同。

4.8.4 颁发新证书时对订户的通告

CA系统提供对证书在线状态查询协议的支持，用户可以通过安徽CA的网站中在线证书查询来获取证书有效性的检查结果。

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：

安徽CA 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

安徽CA通过 LDAP 证书库的方式公开发布变更后的证书，同时在安徽CA网站上在线证书查询中提供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 安徽CA网站上的在线证书查询中查到。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

出现下列情况之一，安徽CA将强制吊销所签发的电子证书：

1. 用户申请电子证书时，提供的资料不真实；
2. 用户没有按照规定缴纳电子证书服务费用；
3. 用户未履行证书服务责任书约定的义务；
4. 用户主体消亡；
5. 用户变更电子证书的用途；
6. 用户要求吊销电子证书

另外，用户也可以提出吊销电子证书的请求；

4.9.2 请求证书吊销的实体

合法的安徽CA证书用户，并需提交身份证明文件（如个人身份证件、企业工商营业执照、组织机构代码证等）

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。终端用户申请撤消是用户提出申请，RA管理员审核，审核通过后，撤消该用户证书。

4.9.4 吊销请求宽限期

如果出现私钥泄露等事件，吊销请求必须在发现泄露或有泄露嫌疑 8 小时内提出，其他原因的吊销请求必须48小时之内提出。

4.9.5 电子认证服务机构处理吊销请求的时限

对吊销的请求电子认证服务机构在24小时内完成吊销请求。

4.9.6 依赖方检查证书吊销的要求

通过安徽CA提供的CRL查看证书状态，以获得用户证书是否可以信赖的信息。

4.9.7 CRL 发布频率

安徽CA可以实时发布和定期在24小时内发布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

通过安徽CA提供的7*24小时的OCSP服务器提供的服务，用户可以使用OCSP客户端工具随时查询其他订户证书的状态。

4.9.10 在线的吊销查询要求

依赖方通过查询安徽CA的CRL来判断证书是否可信。

4.9.11 吊销信息的其他发布形式

OCSP 作为可选的吊销通知形式。

4.9.12 对密钥遭攻击的特别处理要求

证书的私钥泄密，或者怀疑泄密，密钥对已不再用于原来用途的情况下，安徽CA颁发的证书均需吊销停止使用。

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

合法的安徽CA证书用户。

4.9.15 挂起请求的流程

挂起由用户提出申请，并由管理员审核，审核通过后，挂起该用户证书。

4.9.16 电子认证服务机构处理挂起请求的时限

对挂起的请求电子认证服务机构在24小时内完成挂起请求。

4.9.17 挂起的期限限制

挂起的时间不得超过证书的实际有效时间。

4.10 证书状态服务

4.10.1 操作特征

安徽CA 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。安徽CA 的目录服务器系统采用 LDAP 协议，将证书和证书吊销列表(CRL)存放在其中供应用在需要验证身份时查询。安徽CA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，由安徽CA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

安徽CA提供7*24 小时不间断服务。用户可以通过标准的证书状态查询接口来获取证书有效性的检查结果。

4.10.3 可选特征

可以查询证书的持有人及相关信息，证书的使用期限等特征。

4.11 订购结束

订购结束是指当证书有效期满或证书吊销后，该证书的服务时间结束。订购结束包含以下两种情况：

a)证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，视为订购结束；

b)在证书有效期内，证书被吊销后，即订购结束。

对订购结束进行相关操作，应详细记录操作过程，并对其妥善保存。

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

CA 系统密钥的生成，其安全性通过管理手段和技术手段两方面保证。策略上，必须要求超过2名管理员在场的情况下才能进行操作；行为上，加密机管理程序必须对管理员身份进行认证（通过验证管理员IC 卡）。当超过半数的管理员在场并通过身份认证后，启动加密机的管理程序进行加密机的密钥对的初始化生成。

CA 系统的密钥，即加密机中的密钥对，生成后由加密机保存。其中公钥由CA 系统软件从加密机中取出，制作证书等应用，私钥由加密机保护，无法从加密机中取出，如果强行操作，如采用物理攻击手段，加密机的数据将自行破坏。采取以上手段保证根密钥的安全性。加密机初始化生成CA 密钥后应该及时对其使用密钥卡进行备份，一旦加密机中的密钥遭到破坏可以及时得到恢复。

在进行密钥的恢复时，需要半数以上的加密机管理员通过身份认证方可进行。启动加密机的密钥管理程序，从备份的密钥卡中恢复CA密钥。

4.12.2 会话密钥封装和恢复策略与行为

加密机中的密钥通过PKCS#11标准接口由CA系统软件使用。专门用于加密传送信息的密钥即会话密钥，当CA系统软件执行所有与加密机私钥有关的加解密、签名验证运算，均使用会话密钥。策略上，这些过程在加密机内部执行。加密机中的私钥在所有运算过程中不出加密机。

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

安徽CA的建筑物和机房严格按照国家的相关建设规范并经权威部门的验收合格。

安徽CA机房位于安徽省芜湖市镜湖区电信大楼8楼，实行分层访问的安全管理。安徽CA的功能区划分为：入口、办公区、敏感区、服务区、核心区。

5.1.2 物理访问

对支持安徽CA系统的服务设施，如配电盘、通讯与电话间、通风以及空调系统都采取了严格的保护措施，限制人员的随意进入。整个楼宇和机房设备区设有录像监控系统，实行24小时实时监控。

5.1.3 电力与空调

执行连续操作的所有硬件设备室都配备了空调系统及照明系统，同时还考虑了应急环境设施。

市电采用两路供电措施， 并使用UPS提供电力保护。

5.1.4 水患防治

机房内无渗水、漏水现象，主要设备采用专用的防水插座，并采取了必要的

防范措施，防止下雨和水管破裂对设备和设施的影响，安徽CA整个系统有充分保障，能够防止水侵蚀。

5.1.5 火灾防护

安徽CA的电器系统符合电子数据处理设备的防火标准、组织政策、职业安全与保健法等。机房内配备了自动火情警报及处理装置。

5.1.6 介质存储

安徽CA的存储介质包括硬盘、磁带等，介质存储地点和安徽CA系统分开并且保证物理安全，注意防磁、防静电干扰、防火、防水，由专人管理。

5.1.7 废物处理

废弃纸介质实行专人不可还原处理，其他介质以不可恢复原则进行相应的销毁处理。对于硬件设备必须在清空设置后方可搬出中心机房。

5.1.8 异地备份

为了提高灾难恢复的时间和质量及安全信息的保密性，关键数据的备份介质采取异地存放保管的方式。

5.2 程序控制

5.2.1 可信角色

可信角色包括：系统管理员，系统操作员，审核员等。

5.2.2 每项任务需要的人数

安徽CA从安全角度出发，严禁单人进入机房，严禁单人操作。每项操作至少要有两个人参加才可进行。

5.2.3 每个角色的识别与鉴别

所有安徽CA的在职人员，按照所担任的角色的不同进行身份鉴别。进入机房需要门禁卡进行识别；进入系统需要使用电子证书进行身份鉴别。安徽ＣＡ将独立完整的记录其所有的操作行为。

5.2.4 需要职责分割的角色

为保证系统安全，遵循可信角色分离的原则，即可信的角色有不同的人去担任。需要进行指责分割的角色，包括但不限于下列人员：

a)从事证书申请信息验证的人员；

b)负责证书申请、撤销、更新和信息注册等服务请求的批准、拒绝或其他操作的人员；

c)负责证书签发、撤销等工作或者能够访问受限、敏感信息的人员；

d)负责处理订户信息的人员；

e)负责生产、签发和销毁CA系统证书的人员；

f)负责密钥及密码设备管理、操作人员。

对于证书服务的受理，通过录入员、审核员、制证员3个角色才能完成。

对于CA密钥的操作，必须有3名以上的CA密钥管理员同时到场，才能进行有效操作。

5.3 人员控制

5.3.1 资格、经历和无过失要求

安徽CA要求CA运行管理人员具有本科及本科以上学历，有系统维护经验及网络安全经验的人。无不良的爱好，同时具有很好的协调能力、团队合作能力。

另外安徽CA对CA运行管理人员的背景、资历、经验等情况都进行了必要的核实和审查。

5.3.2 背景审查程序

安徽CA对应聘CA运行管理人员背景的审查程序为：

（1）人力资源部负责对应聘人员的个人资料予以确认。系统管理员、操作员和审核员应提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。

（2）办公室通过电话、信函、网络、走访、调阅档案等形式对其提供的材料的真实性进行鉴定。

（3）用人部门通过现场考核、日常观察、情景考验等方式对其考察。

（4）所有人员需要提供由公安部门出具的无犯罪证明，经主管领导批准后方可上岗。

5.3.3 培训要求

定期对操作人员进行技术培训，减少因系统操作人员的操作错误造成系统故障。

对于中心的所有员工进行不定期的安全意识教育和培训，增加责任感。

对员工的技术提升，不定期的提供各种参加培训的机会和实践

5.3.4 再培训周期和要求

安徽CA制定了一整套严格的再培训制度并将严格执行，对再培训的效果由各岗位负责人员及人力资源部共同进行考核，考察再培训后的效果。

5.3.5 工作岗位轮换周期和顺序

按照各区之内到各区之间轮换的方式对工作岗位进行轮换。具体情况按照员工的工作时间工作经验调整。

5.3.6 未授权行为的处罚

在操作规则方面包括以下内容：

1．为每个操作人员签发一张电子证书并建立相应的访问控制权限表（ACL）防止对系统的非授权操作。

2．定期对操作人员进行技术培训，减少因系统操作人员的操作错误造成系统故障。

3．对于软盘、光盘等设备的使用进行严格限制，未经安全管理人员的同意不得使用。

4．严禁在安徽CA系统机器上执行无关的工作，特别是对于安徽CA的签发服务器和RA 的注册服务器，以免对系统的安全造成威胁。

如果违反，按照保密协约的要求进行处罚。

5.3.7 独立和约人的要求

安全方面，对于所有的人员要求是一样的。而且，不安排其接触系统核心软/硬件及网络设施。

5.3.8 提供给员工的文档

为保证系统的正常运行，安徽CA根据不同的角色提供给管理员一些技术性文档：

- ✧ 各岗位日常操作手册
- ✧ 安徽CA电子认证业务规则
- ✧ 系统恢复操作手册等

5.4 审计日志程序

安徽CA的审计日志由运维部门统一保存，定期备份，备份介质分别存放在安徽CA及异地存储中心。一旦出现审计纠纷，需要对审计日志提出复查，应由客户向市场部申请，经总经理同意后，由运维人员查询。

5.4.1 记录事件的类型

在安徽数据库中的记录事故类型包括：

- ✧ 创建CA 签字密钥对
- ✧ 在系统中增加和删除最终用户
- ✧ 为所有的安徽CA用户变更加密密钥对历史及公钥校验历史，包括证书发

布和撤消事项

- ✧ 改变最终用户DN
- ✧ 增加和消除安徽CA 管理员和安全官员特权
- ✧ 变更安全专家特权
- ✧ 改变政策的一些方面例如证书的有效期

5.4.2 处理日志的周期

每两周至少进行一次审记跟踪处理(检查违反政策及其它重大事件)。

5.4.3 审计日志的保存期限

审计日志每月形成新的归档文件，交由相关部门保存归档，审计跟踪文档至少保存二年，密钥和证书信息档案至少保存到证书失效后5年。

5.4.4 审计日志的保护

将审计日志存贮到计算机外的安全介质中，并专人安全保管。定期查询审记日志。

5.4.5 审计日志备份程序

审记文档由管理员每月进行一次归档。所有文档包括最新的审记跟踪文档需储存在磁盘中并存放在安全的文档库内。

5.4.6 审计收集系统

审计资料的收集由安徽CA和RA 系统以及CA 和RA 管理员完成。

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

根据对归档日志的处理结果进行分析，对发生问题的频率和解决时间进行记

录，从而评估其脆弱性。

5.5 记录归档

日志记录由系统定期归档，由运行人员每周复查，每月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

安徽CA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

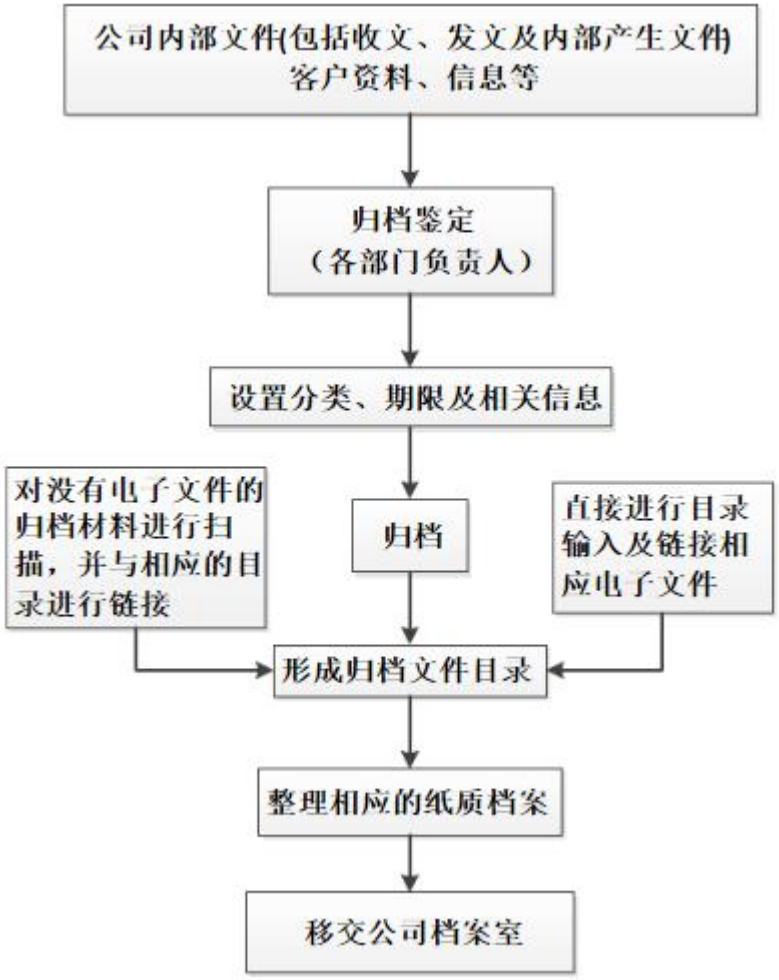
面向企事业单位、社会团体、社会公众的电子政务电子认证服务，归档信息保存期为证书失效后五年；面向政务部门的电子政务电子认证服务，归档信息保存期为证书失效后十年。其他归档记录一般规定保存期限为证书失效后五年。

5.5.3 归档文件的保护

将归档文件存贮到计算机外的安全介质中，并每月在异地进行备份，异地指公司不同地市的经营场所保险柜或者银行保险柜。定期查询登记日志。备份保存在有安全控制的房间内，要求在防潮湿、防静电感应的环境下。没有授权的人员无法访问和更改。为防止介质老化，应定期性将数据的可用性进行检查。

5.5.4 归档文件的备份程序

记录文档由管理员每月进行一次归档。所有文档包括最新文档需储存在磁盘中并存放在安全的文档库内。



5.5.5 记录的时间戳要求

归档的记录都需要标注时间；按照操作的实际时间进行记录。

5.5.6 归档收集系统

归档内容由证书系统内部控制。

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

进行密钥更新时，密钥管理中心首先为用户生成新的密钥对，然后将新的密

钥对安全地备份到数据库中，接下来将新的密钥对以安全地方式发送给认证中心，以签发包含新密钥的新证书，最后，对旧的密钥进行归档和销毁。

包括以下几个操作：

1）新密钥的生成与分发

2）新密钥的备份

3）旧密钥的归档（密钥历史信息的保存）

4）旧密钥的销毁

5.7 事故与灾难恢复

5.7.1 事故和损害处理流程

遇到突发事故和损坏，如火灾等需要利用灭火设施处理现场，再进行其它的软硬件及数据的恢复。

安徽CA制定了灾难恢复方案。

5.7.2 计算资源、软件和/或数据的损坏

防火墙、路由器、交换机的恢复：执行防火墙、路由器和交换机的相关命令和软件备份防火墙、路由器和交换机的配置文件。

数据库恢复的过程是数据备份的逆过程，它们的数据流向不同。

5.7.3 实体私钥损害处理程序

实体私钥损害后无法为用户恢复，处理的程序：

(1)确定实体私钥是否真的损害

(2)确实损害，在PKI 系统使用中提取密钥管理中心的原有证书的加密密钥为用户申请新的证书。

这样对于原来的加密的数据用户仍旧可以使用。

5.7.4 灾难后的业务连续性能力

灾难恢复后安徽CA仍旧保持日常的8小时证书申请能力和24小时证书状态查

询及CRL查询能力。

5.8 电子认证服务机构或注册机构的终止

将按照国家的相关法律及规定执行。

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

CA系统：CA系统密钥的生成，是当超过半数的管理员在场并通过身份认证后，启动加密机的管理程序进行加密机的密钥对的初始化生成。

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。

6.1.2 私钥传送给订户

将密钥加密密钥的产生算法及保护用户密钥的加解密算法程序一并发给用户。

6.1.3 公钥传送给证书签发机构

用户通过安全软件把公钥通过安全通道发给安徽CA以便安徽CA生成证书。

6.1.4 电子认证服务机构公钥传送给依赖方

安徽CA会把自己的公钥通过安全软件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安徽CA的信息。

6.1.5 密钥的长度

安徽CA用户签名、加密密钥对支持2048/1024 RSA

安徽CA用户签名、加密密钥对支持256 SM2

6.1.6 公钥参数的生成和质量检查

安徽CA系统的密钥中公钥由CA系统软件从加密机中取出，其质量由加密机决定。

6.1.7 密钥使用目的

密钥的用途在证书的“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 密码模块标准和控制

安徽CA的密码模块使用加密机密码模块，采用四川卫士通网络安全有限公司生产的加密机，安置在安全区。并在有至少两名管理员在场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分别同时拥有三张管理员口令卡片、备份卡，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员负责掌握，一旦需要使用，必须经过运行部负责人与安全员共同申请，由首席安全官签字后方能使用。使用时运行部负责人必须在场，不得随意复制，使用后交还安全员保管，使用前后必须登记。

安徽CA私钥的备份数据以光盘的形式存放在保险柜中，如有特殊情况需要使用，必须经过运行部门负责人与安全员共同申请，由首席安全官签字。负责保险柜的管理员将对应的安徽CA私钥备份文件交给使用人，使用时必须由运行部负责人和使用人同时在场，严禁复制，使用完毕后由运行部门负责人亲自将数据销毁。

6.2.2 私钥多人控制（m 选 n）

实现2OF3的机制，必须有2人到场的情况才能对加密机操作。

6.2.3 私钥托管

CA 系统的密钥，其中私钥由加密机保护，无法从加密机中取出，如果强行操作，如采用物理攻击手段，加密机的数据将自行破坏。采取以上手段保证根密钥的安全性。

由KMC密钥中心为用户生成的加密密钥对放置在KMC密钥托管库中。

6.2.4 私钥备份

作为灾难恢复的一项措施，需要进行密钥备份。安徽CA采用四川卫士通网络安全有限公司的加密主机对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。

6.2.5 私钥归档

作为灾难恢复的一项措施，必须进行密钥归档。不再使用的私钥，由运行部人员操作，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。对用于安全传输的密钥，在进行密钥更新时，为了保证以前加密的数据不丢失，需要对用于解密的私钥进行归档。存档的时间由系统的安全策略决定。归档后的密钥形成历史信息链，供用户查询或恢复。进行密钥归档时，密钥管理中心从备份数据库中取出要归档的用户密钥，然后将它们安全地存入归档数据库，并插入对应的历史信息链中，供以后用户恢复及查询，同时密钥管理中心还将备份数据库中该密钥的备份删去。

6.2.6 私钥导入、导出密码模块

安徽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

密钥加密密钥（包括了私钥）采用主密钥加密后保存到密钥管理中心的数据

库或带密码运算的加密IC卡中，并进行备份，这样在司法取证等情况下，可以通过主密钥恢复密钥加密密钥。

6.2.8 激活私钥的方法

具有激活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，进行激活私钥的操作，需要至少2名管理员同时在场。

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，需要至少2名管理员同时在场。

6.2.10 销毁私钥的方法

安徽CA的私钥不再被使用，或者与私钥相对应的公钥到期或者被撤销后，加密设备必须被清空。同时，所有用于激活私钥的PIN码、IC卡、动态令牌等也必须被销毁或者收回。销毁时由3名以上的密钥管理员共同在场，由操作员负责清空硬件加密设备，完成密钥销毁。私钥归档的操作按照本CPS的规定处理。

6.2.11 密码模块的评估

安徽CA使用的加密机是通过国家密码管理局鉴定并批准使用的四川卫士通网络安全有限公司生产的具有自主知识产权的高速主机加密设备。该系列加密机密码模块的设计要达到以下标准：

标准化，支持密码算法、密钥格式、加密、解密、签名运算模式都符合国际或国家标准。可扩充，即密码系统通过模块化设计，可以动态增加密码算法的种类，在统一的开发接口下，增加新的密码算法，对密码算法的强度也可以选择。强安全，即密码系统必须安全的管理密钥，对密钥有安全的备份，控制密钥的访问权限，生成的密钥有足够的强度。高可靠，即密码系统有高的可靠性，能保证密码运算的正确性。在公钥系统中，密钥的质量符合标准，运算速度达到应用系统目标，并提供不间断服务。

6.3 密钥对管理的其它方面

6.3.1 公钥归档

公钥由CA系统软件从加密机中取出制作证书时使用，归档在CA系统数据库中。

6.3.2 证书操作期和密钥对使用期限

所有订户的证书有效期和其对应的密钥对俄有效期是一致的。

6.4 计算机安全控制

6.4.1 特别的计算机安全技术要求

安徽CA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：

系统安全配置，关闭不必要的服务与端口。

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。

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。

各人负责各自权限范围内的操作。

日志和操作记录的审计制度。

数据备份和恢复机制。

6.4.2 计算机安全评估

安徽CA系统已经通过国密办组织的安全性审查。

6.5 生命周期技术控制

6.5.1 系统开发控制

在系统开发过程中，安徽CA在安全的开发环境下，严格按照软件工程的要求

进行开发控制。系统是PKI 的核心组成部分，主要有：

验证并标识证书申请者身份。

确保CA 用于签名证书的非对称密钥的质量。

确保整个签证过程的安全性，确保签名私钥的安全性。

证书资料信息（包括公钥证书序列号、CA 标识等）的管理。

确定并检查证书的有效期限。

确保证书主体标识的唯一性，防止重名。

发布并维护作废证书列表。

对整个证书签发过程作日志记录。

6.5.2 安全管理控制

在管理控制方面按以下规则进行：

1．为每个操作人员签发一张电子证书并建立相应的访问控制权限表（ACL）防止对系统的非授权操作。

2．定期对操作人员进行技术培训，减少因系统操作人员的操作错误造成系统故障。

3．对于软盘、光盘等设备的使用进行严格限制，未经安全管理人员的同意不得使用。

4．严禁在CA系统机器上执行无关的工作，特别是对于CA的签发服务器和RA的注册服务器，以免对系统的安全造成威胁。安徽CA对CA 系统的维护保证操作系统、网络设置和系统配置安全。通过日志检查来检查系统和数据完整性和硬件的正常操作。

6.5.3 生命期的安全控制

生命期间保证CA签名密钥、加密密钥及相关密钥的安全，密钥保存在加密机中，专人管理，并采用了2 OF 3的机制进行控制。

6.6 网络的安全控制

在安徽CA的网络系统中，把整个网络划分为三个区：操作区、DMZ和核心安

全区。各安全层次之间采用不同类型的防火墙，每个安全层次在一个子网上，安全策略不尽相同，使得网络系统具备很强的防范能力。

在采用多层防火墙技术增加系统的安全性的同时，我们还选用了清华同方公司的网络安全系列产品，这些产品可以从多方面对网络系统进行监测和分析，能够及时发现入侵者并及时报警，同时还能够采取一定的补救措施。

安徽CA系统的 软件加密模块的设计符合FIPS140-1 一号标准。

6.7 时间戳

用户在使用时间戳时需要权威的时间源。文档上的时间戳涉及对时间和文档内容的哈希值。权威的签名提供数据真实性和完整性。安徽CA提供的时间源服务采用的是中国授时中心提供的标准时间源，可以为用户提供安全可靠、标准的时间戳服务。

7 证书、证书吊销列表和在线证书状态协议

7.1 证书

7.1.1 版本号

安徽CA证书格式符合X.509 V3 标准，并可以提供支持证书扩展的能力。

7.1.2 证书扩展项

证书扩展项即证书扩展部分。包括证书签发者的甄别名，签发证书序列号，用户主体的公钥标识，CRL发布，证书公钥用途，用户私钥有效期，安徽CA承认的证书政策列表，用户主体目录属性，CA签名算法标识等。

7.1.3 证书标准项

（1）电子认证服务提供者名称；

（2）证书持有人名称；

（3）证书序列号；

（4）证书有效期；

（5）证书持有人的电子签名验证数据；

（6）电子认证服务提供者的电子签名。

7.1.4 算法对象标识符

算法：

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

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

签名/摘要算法：MD2、MD5、SHA1。

7.1.5 名称形式

安徽CA证书通过DN来命名。

DN 的具体内容依次由CN、OU、O、L、S、C 六部分组成。其中:

CN用来表示用户名，

OU为组织单元

O为组织名称

L为地市名称

S为省市名称

C为国家名称，这里等于CN,指中国。

7.1.6 名称限制

在DN 中，可以使用除专用字符（“\” 和“″”）和特殊字符（“，” 、“=” 、“+” 、“#” 、“<” 、“>” 、“;” ）外的多数ASCII 字符。

7.1.7 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电子证书。

7.1.8 策略限制扩展项的用法

规定在CA体系中的各层CA使用相同的CP以及是否和其他CA体系互相信任。
安徽CA未使用本扩展域。

7.1.9 策略限定符的语法和语义

Certificate Policies CA 证书政策列表
Policy Mappings 策略映射
Basic Constraints 基本制约
安徽CA未使用本扩展域。

7.1.10 关键证书策略扩展项的处理规则

安徽CA未使用证书策略扩展项。

7.2 CRL

7.2.1 版本号

安徽CA使用的CRL符合X.500 标准。

7.2.2 CRL 和 CRL 条目扩展项

CRL 数据定义：
（1）版本（Version）
含义：显示CRL 的版本号。
（2）签名（Signature）
含义: 签发CRL 的CA 的签名。
（3）算法标识（algorithmIdentifier）
含义:定义签发CRL 所使用的算法。

（4）CRL 的签发者（Issuer）

含义:指明签发CRL 的CA 的甄别名。

（5）CRL 发布时间（thisUpdate）

（6）预计下一个CRL 更新时间(next update)

（7）吊销证书信息目录(revoked certificates)

（8）CRL 扩展（CRL Extension）

CA 的公钥标识(AuthorityKeyIdentifier)

CRL 号（CRL Number）

7.3 在线证书状态协议

7.3.1 版本号

安徽CA可以提供支持RFC2560(X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP)的版本1.0 的OCSP 服务。

7.3.2 OCSP 扩展项

采用标准扩展，基于X.509 版本3 证书所使用的扩展模型，主要有：

(1) 随机数(Nonce)

(2) 证书吊销列表参考(CRL References)

(3) 可接受的回复类型(Acceptable Response Types)

(4) 证书吊销列表项目扩展(CRL Entry Extensions)

(5) 服务定位器（Service Locator）

8 认证机构审计和其它评估

8.1 评估的频率或情形

安徽CA的评估根据情况而定，有年度评估、运营前评估、安全事件发生后的评估和随时进行评估。

8.2 评估者的资质

评估人员应具备PKI 和CA 系统基本知识，熟悉行业规范，具有行业相关知识或者具有国家评估审计人员相应资质。

8.3 评估者与被评估者的关系

为了保障评估的公正性，评估者与被评估者应无任何业务、财务往来或其它利害关系足以影响评估的客观性。

8.4 评估内容

安徽CA审计按审计客体分为内部审计和外部审计。内部审计由安徽CA的内部审计部门来承担，外部审计由安徽CA委托第三方审计机构来承担。安徽CA审计遵循审计的独立性、权威性、客观性、公正性、政策性、针对性、群众性、重要性、保密性和稳健性的原则。评估参照的规范和标准有BS7799 和ISO9000 等。

评估认证中心的日常行为操作步骤

- 证书生成的流程
- 密钥有关的各项内容
- 系统维护与开发
- 岗位说明和各项操作手册，安全制度
- 协调所有的相关岗位

8.5 对问题与不足采取的措施

提出当前各种评估内容存在问题的报告，由会议讨论，经过组织权威和操作权威的审定后，重新修订现有的资料及其策略，使新的技术方案得到妥善解决和实施，并通知下级实体正确维护操作。

8.6 评估结果的传达与发布

评估结果可以根据具体情况公布给被评估方、其它方和公众。

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

安徽CA采用政府主导，企业运营的运行机制，向社会各界提供服务的同时，按照“有偿服务、不以赢利为目的”的原则，对电子证书的发放、验证和管理实行有偿服务，用户有义务按照规定向安徽CA交纳相关服务费用。

安徽省物价管理部门已正式批准了安徽CA电子证书相关费用。安徽CA已在公司的网站（Http://www.aheca.cn）上予以发布。根据证书实际应用的需要，安徽CA在不高于此价格的前提下可以对证书价格进行适当调整。费用变化情况安徽CA将通过网站以及其它适当方式予以发布。

9.1.2 证书查询费用

安徽CA保留对用户证书查询操作进行收费的权利。

9.1.3 证书吊销或状态信息的查询费用

安徽CA保留对用户证书吊销和状态信息查询操作进行收费的权利。

9.1.4 其它服务费用

安徽CA保留收取其他服务费的权利。

9.1.5 退款策略

在安徽CA依照用户提交的资料正确制作证书前提下，用户对所收到的安徽CA签发的电子证书予以确认后，安徽CA不办理退证、退款手续。在用户已经交纳服

务费期间，用户要退出安徽CA电子证书服务的，安徽CA不退还剩余使用时间的服务费。

9.2 财务责任

对于操作中涉及的其它用户财务相关信息的保险，例如财务报表、担保合同、信用证明和各种权益证明，目前没有开设相应险种。

对于终端用户由于使用安徽CA证书服务造成的事故的保险和担保目前没有开设相应险种。 由于没有开设相应险种，目前没有保险。

9.3 业务信息保密

安徽CA根据国家相应的法律法规制定并落实严格的信息保密规章制度，所有相关人员（包括安徽CA及其业务代理机构的工作人员、证书持有者）必须遵守该规章制度。由安徽CA制定及实施的信息保密规章制度符合国家保密机构的相关规定。安徽CA有权根据情况修改相关内容。

除非有法律明确规定和要求，有关递交证书申请的用户信息将由安徽CA保密并且在没有得到申请人授权的情况下不得泄露。这不适用于证书中、或由安徽CA来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、贸易机密等按照保密协议进行保密。

除非有法律明文规定，安徽CA没有义务公布或透露用户所持有证书以外的信息。

9.3.1 保密信息范围

以下信息应视为保密信息但不限于以下方面：

安徽CA用户的数字签名及解密密钥，并且CA 和RA 均无权访问这些密钥。

保存在审计记录中的信息应由安徽CA保密，除受法律要求，不可在公司外部发布。审计记录包括：本地日志、服务器日志、归档日志的信息，应对安徽CA可视为保密，只有审计员和首席安全官员可以查看。除法律要求，不可在公司外部发布。年度审计结果也同样视为保密。

除去作为证书的、CRL、和证书策略或本CPS 一部分而公开出版的信息，其他由CA 和RA 保存的个人和公司信息应视为保密，除法律要求，不可公布。

在双方披露时标明为保密（或有类似标记）的、双方根据合理的商业判断应理解为机密数据和信息的、以其他书面或有形形式确认为保密信息的或从上述信息中衍生出的信息，也视为保密信息。

其他：安徽CA信息的保密性取决于特殊的数据项和申请。

9.3.2 不属于保密的信息

以下信息可视为不保密信息

由安徽CA签发公钥证书和CRL 中的信息。

由安徽CA支持的证书策略中信息。

安徽CA许可，只有安徽CA用户方使用，在安徽CA网站公开发布的信息。

用户证书撤消原因可以在撤消证书的CRL 入口查到。其中撤消原因不视为保密信息，可为所有安徽CA用户和可靠用户共享。

其他可以通过公共渠道获得的信息。

当安徽CA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电子认证业务规则中具有保密性质的信息时，安徽CA可以依从法律、法规或规章条款以及法院的判定的要求，向执法部门公布相关的保密信息。此种信息披露不视为违反了保密的要求和义务。

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并保证不泄露给第三方的责任。

9.4 个人信息私密性

9.4.1 隐私保密方案

个人私密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

与证书持有者公钥配对的私钥是保密的，证书持有者应当妥善保管，不得泄漏或交付他人。如因故意、过失导致他人知道或遭盗用、冒用、伪造或者篡改，证书持有者应当自行负责承担一切责任。

用户在申请电子证书时提供的存在于CA、RA 和数据库中的私人信息，包括申请办理人的联系电话、电子邮件地址和通信地址等信息，安徽CA视为保密的个人信息，如非必要不可泄露。

9.4.3 不视为隐私的信息

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，通过安徽CA目录服务等方式向外公布。

9.4.4 保护隐私的责任

个人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。

9.4.5 使用隐私的告知与同意

在授权下可以使用私密信息;在政府管理和司法程序要求下有权使用私密信息。

9.4.6 其它信息披露情形

当保密信息的所有者出于某种原因，要求安徽CA公开或披露其所拥有的保密信息，安徽CA应当满足其要求。如果这种保密信息的披露行为涉及或有可能引起对其他方的赔偿义务，安徽CA有权拒绝其要求，且不应该承担任何由此相关的或由于公开保密信息引起的损失和损坏的赔偿责任。保密信息的所有者应负责安徽CA与此相关的或由于保密信息公开引起的损失和损坏的赔偿责任。

9.5 知识产权

安徽CA享有并保留对证书以及安徽CA提供的全部软件的独一无二的一切知识产权，包括（所有权、名称权、利益分享权等）。

安徽CA对电子证书系统软件具有所有权、名称权、利益分享权。

安徽CA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联互通。

安徽CA网站上公布的一切信息均为安徽CA财产，他人不能转载用于商业行为。

安徽CA签发的证书、CRL、提供的软件、相关的文件和使用手册均属于安徽CA的知识产权范围。

安徽CA电子认证业务规则为安徽CA财产。

在没有安徽CA预先书面同意的情况下，证书持有者不能在任何证书到期、废止、或终止的期间或之后，使用或接受任何安徽CA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。

证书申请人（于接受申请时即为用户） 声明并保证其交付（给安徽CA） 使用的网域与辨识名称（及所有其它证书申请书的资料）不得在任何管辖区域内干预或侵犯第三人的商标、服务标志、商标名称、公司名称或其它知识产权等权利，而且不用于非法目的，包括侵害、干扰协议或预期的商业利益、不公平竞争、损害他人信誉及干扰或误导他人。证书申请人（于接受申请时即为用户）应为安徽CA辩护、赔偿并使其不受此类干扰或侵权而造成损失或损害赔偿。

9.6 陈述与担保

9.6.1 安徽 CA 的陈述与担保

安徽CA享有的权利主要有以下方面：

① 要求电子证书申请者提供真实资料的权利，有权按申请不同类型的电子证书，要求申请者提供不同的真实资料：对个人电子证书申请者、单位电子证书申请者、服务器电子证书申请者要求提供的有关资料参见安徽CA电子证书申请表

的相关内容（申请表可以从安徽CA网站、受理点等处获得）。安徽CA或安徽CA授权的受理审核单位在遵循合法程序的前提下有权对上述内容进行调查、审核。

② 根据业务发展的需要，有权委托相关法人单位作为业务受理审批单位（即业务受理点）从事电子证书的受理、电子证书用户的身份审核和发放等。

③ 有权提供不同类型的电子证书，满足不同的电子证书用户的不同需要。

④ 安徽CA有权向证书申请者颁发证书、撤销证书、发布证书注销列表等对证书操作的一系列流程，并为安徽CA制定出相关的规则。

⑤ 安徽CA有权根据国家相应的法律制定安徽CA法律责任书，并有权让证书用户遵守安徽CA的规定。

⑥ 安徽CA有权制定服务责任书，并有权让证书用户遵守安徽CA的规定。

⑦ 收取费用的权利：安徽CA有权向证书申请者按安徽省物价部门核准的价格收取费用。

⑧ 安徽CA在法律许可范围内有权对所有电子证书遭受破坏或盗用的情况协助调查，其调查包括但不限于面谈、记录与相关程序、相关设施的检查等。

⑨ 安徽CA对于下列情况之一，将有权主动废止所签发给证书持有者的证书：

◆ 证书申请初始注册时，提供不真实材料；

◆ 违反国家法律或者其它规章制度，不应签发证书的；

◆ 有盗用、冒用、伪造或者篡改他人证书的；

◆ 不履行安徽CA的服务规范，如本电子认证业务规则中的规定；

◆ 与证书中的公钥相对应的私钥被泄密；

◆ 证书中的相关信息有所变更；

◆ 由于证书不再需要用于原来的用途而要求终止；

◆ 用户未履行证书更新手续（该手续包括提出证书更新的书面申请，以及按规定缴纳相关费用）。

◆ 其他情况。

⑩ 安徽CA有权确认：证书申请人确为证书申请书所说明的实体（依据证书类型描述的内容）； 证书申请人合法地持有证书中所列的公开密钥所对应的私人密钥；除未经证实的证书用户资料外，证书中所记载的资料均准确无误，任何申请列有证书申请人公开密钥的证书的代理人是经过合法授权提出申请的。

当使用或信赖证书的证书依赖方或安徽CA的业务代理机构和雇员的违约行为或其他行为导致安徽CA发生任何损失、损坏或债务责任和法律费用以及成本损耗，安徽CA有权要求赔偿。

安徽CA对所担负的法律规范的有限责任做出如下承诺：

① 安徽CA的运作遵守《中华人民共和国电子签名法》等法律，接受国家和地方信息产业主管部门和密码管理主管部门的领导。

② 为进行网上业务的各方提供信息安全基础设施，并且经过国家有关管理机关鉴定和审批，合法许可经营。

③ 建立和执行符合国家政策的规定的安全机制，管理所拥有的信息安全基础设施并使其处于良好运行状态，并使安徽CA的签名私钥在安徽CA内部得到安全的存放和保护。

④ 对申请证书登记人的身份进行严格的审查和认证，保证发放的证书具有可靠的权威性和信任度，保证电子证书的真实有效性，即所发放电子证书中的公共密钥同某个确定身份的人是一一对应的。

⑤ 安徽CA有告知的责任，应向社会公开披露以下内容并保证该内容的准确完整：

一是根证书；二是电子证书上所列明的数字信息；三是用户的公钥；四是认证业务操作规范（CPS）；五是废止名单（CRL）。

⑥ 负责证书签发和管理，包括控制实际的证书产生过程，证书的发布，证书的注销和证书的更新；及负责确保根据本电子认证业务规则的要求说明和做好与证书有关的服务、操作等各方面的工作。

⑦ 遵守安徽CA电子认证业务规则的规定，做好电子认证业务规则的版本管理与控制，对修订后的电子认证业务规则及时予以发布。

⑧ 安徽CA承诺使用安徽CA提供的电子证书与安全软件的用户的网上交易信息对无关者是保密的，而且在网上传输中是不可篡改的。

⑨ 安徽CA承诺在现有技术条件下，除非安徽CA私钥丢失，安徽CA签发的电子证书不会被成功地伪造、篡改；如果由于安徽CA的私钥管理问题造成电子证书被伪造、篡改，安徽CA将承担相应责任。

⑩ 安徽CA承诺在现有技术条件下所采用的密码机制无法攻破。如果发生电

子证书密码机制问题，而安徽CA没有及时采取应对措施，安徽CA将承担责任。

除上述的责任条款，安徽CA、安徽CA的服务机构、安徽CA的授权发证机关、安徽CA的雇员不做任何其他保证和履行任何进一步的义务。

需要明确的是，本电子认证业务规则的内容，没有任何信息可以暗示或解释为安徽CA必须承担其它的义务或安徽CA必须对其行为做出其它的承诺。

9.6.2 RA 的陈述与担保

RA 的职责是：

① RA 应遵守由安徽CA制定的所有运营政策、操作管理规范、规定登记程序和安全保障措施。安徽CA有权根据情况修改有关内容。

② RA 有责任验证申请人提供信息的准确性和可靠性。验证过程由RA 审核执行，通过安徽CA制定的审核步骤，确定颁发的证书的有效性和真实性。

③ 承担发布CRL 并保证CRL 准确性与及时性的责任。

④ RA 应使用安徽CA确定的信息传输协议和标准，与安徽CA交换信息。

⑤ RA 应承担因在CPS 规定的用途外使用RA 管理员证书所造成的损失的责任。

⑥ 对于安徽CA提供的属于安徽CA专有的技术、软件开发包只有使用权，并对其承担保密义务。无权将未经安徽CA授权的属于安徽CA独有的技术/产品以任何方式让第三方知道和使用，并应对泄密承担相应责任。

9.6.3 受理点的陈述与担保

受理点的职责是：

① 严格遵守安徽CA制定的所有运行策略、操作管理规范和安全保障措施。

② 受理电子证书业务，包括证书申请、证书注销、证书恢复、证书更新。

③ 审核用户信息的真实性及用户身份的真实性。

④ 保障电子证书发放的正确性。

⑤ 承担因工作人员操作失误对用户造成直接经济损失所应承担的相应责任。

⑥ 严密保守客户及公司的商业秘密和技术秘密。

9.6.4 证书持有者的陈述与担保

证书持有者（或证书用户）是安徽CA的客户，是接受电子认证服务的一方。

证书持有者应享有以下权利：

① 获得有效合格的电子证书的权利：证书持有者在提供了符合要求的信息资料并交纳证书服务费用后，有权利取得有效的、具有所需功能的电子证书。

② 提出中止或废止电子证书的权利：在前述的有关安徽CA应该中止或废止电子证书的条件下，证书持有者或其代理人有权提出中止或废止证书的申请。

证书持有者负有以下责任：

① 证书持有者对其私钥应保持控制，采取合理的预防措施避免遭受破坏或盗用，并不得向未经授权的人泄露，确保私人密钥的安全，以防止任何遗失、泄漏、修改或密钥的未经授权使用。因私钥的不安全控制而造成的损失，由证书持有者承担。

② 如果证书持有者的私密钥出现问题，例如遗失、盗用、破坏或者泄密等，证书持有者应当在察觉后的第一时间内通知所有所能预见到的受证书影响的单位及个人，包括安徽CA；同时向安徽CA申请中止或废止该证书。

③ 证书用户（即证书持有者）在申请证书时应真实陈述安徽CA颁发证书时要求其提供的事项，提供真实准确的信息作为证书申请材料。证书持有者应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信息侵犯他人权利而造成后果的责任。

④ 证书持有者应向安徽CA按时交纳服务费用以享受相关服务。

9.6.5 证书依赖方的陈述与担保

① 证书依赖方须熟悉本电子认证业务规则以及和证书持有者证书相关的证书政策，还须了解和遵守证书的使用目的。证书依赖方必须确保证书的确用于预定的目的。

② 证书依赖方在信赖证书持有者的证书前，必须根据相应的最新的证书废止列表（即CRL）检查证书的状态，查明证书是否还在有效期内。

③ 当证书依赖方在网上进行电子商务时，有权审查自己或对方的证书是否在有效期内，是否已被列为“黑名单”，证书依赖方应该在做出决定是否相信某

个证书之前，应该先查看“查询证书”以确定该证书是否为有效的、未经废止的或更新的证书，然后再用该证书来确认该电子签名是否在证书有效期内，是否与证书中所列的公开密钥相对应的私人密钥所产生的，加入电子签名的信息未被改动。必要时有权向安徽CA联系和查询。

9.6.6 其他参与者的陈述与担保

具有与依赖方同样的责任与义务。

9.7 有限责任与免责条款

9.7.1 特定责任的排除

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

对于由于电子证书、数字签名或根据安徽CA电子认证业务规则而提供或设计的任何其他交易或服务的使用、签发、授权、执行或拒绝执行而导致的或与之有关的任何间接性的、特别性的、附带性的、或结果性的损失，或任何利益损失、数据丢失，或其他间接性的、结果性的或惩罚性的损失，无论是否可以合理预见，安徽CA将不会对此承担任何责任。

9.7.2 免责条款

① 安徽CA不对由于客观意外或其它不可抗拒力事件造成的操作失败或延误承担任何损失、损坏和赔偿责任。

② 安徽CA在签发电子证书之前，事先就与证书申请者签定电子认证服务协议，都有事先告知证书持有者的免责条款规定：安徽CA发放的各类型电子证书只能用于在网络上标识身份、加密数据、签名认证、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，不承担任何形式的担保和义务，包括：任何销路担保；保证一定适用于特定目标的担保；以及提供的任何相关信息的精确性的承诺，和所有由于缺乏妥善管理和疏忽引起的责任。若证书持有者将其电子证书用于其他用途，安徽CA不承担任何责任。

③ 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，而他又根据正常的流程提供了必须的审核文件，由此得到了安徽CA签发的电子证书，由此引起的经济纠纷由证书申请者全部承担，安徽CA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。

④ 与证书持有者公钥配对的私钥是保密的，证书持有者应当妥善保管，不得泄漏或交付他人。如因故意、过失导致他人知道或遭盗用、冒用、伪造或者篡改，证书持有者应当自行负责承担一切责任。

⑤ 安徽CA在进行身份认证或证书持有者下载电子证书时，将充分遵守安徽CA的安全操作流程。如果由于非安徽CA自身的原因而造成的安徽CA设备故障、线路中断，导致签发电子证书错误、延迟、中断或者无法签发，安徽CA不负任何赔偿责任。

⑥ 安徽CA仅仅提供电子沟通或交易中签名的“不可抵赖”的依据，但并不对此承担法律责任等方面的约定。

⑦ 当安徽CA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电子认证业务规则中具有保密性质的信息时，安徽CA可以依从法律、法规或规章条款以及法院的判定的要求，向执法部门公布相关的保密信息。此种信息披露不视为违反了保密的要求和义务。

⑧ 当保密信息的所有者出于某种原因，要求安徽CA公开或披露其所拥有的保密信息，安徽CA应当满足其要求。如果这种保密信息的披露行为涉及或有可能引起对其他方的赔偿义务，安徽CA有权拒绝其要求，且不应该承担任何由此相关的或由于公开保密信息引起的损失和损坏的赔偿责任。保密信息的所有者应负责安徽CA与此相关的或由于保密信息公开引起的损失和损坏的赔偿责任。

⑨ 安徽CA不对交叉认证的其他CA 私钥遭到泄露、破坏而造成的损害承担任何赔偿责任。

⑩ 安徽CA不承担任何其他未经授权的人或组织以安徽CA名义编撰、发表或散布不可信赖的信息所引起的法律责任。

若证书主体提交的并最终列入证书中的信息侵犯了他人的专利、商标、著作权、商业秘密或其他知识产权及其他任何权利， 安徽CA不承担任何责任。

安徽CA用户电子证书的有限期为一年，自用户申请之日起计算。用户必

须在证书失效前20 天向CA 中心或受理点提出证书更新请求，否则证书到期后将自动失效，安徽CA不对因用户使用被取消或过期证书而造成的损害承担任何责任。

如证书用户出于某种原因不希望继续使用电子证书时，应当立即到当地证书受理点申请废除电子证书。废除手续遵循各受理点的规定。安徽CA在接到废除申请后，在24小时之内正式废除用户的电子证书。安徽CA不对电子证书正式废除前造成的损害承担任何责任。

9.8 赔偿

9.8.1 理赔

9.8.1.1 安徽 CA 赔偿责任的限制

在安徽CA违反了前文9.6.1 款条例规定的职责，安徽CA承担赔偿责任（法定的或约定免责除外）。赔偿责任的限制如下：
安徽CA所有的赔偿义务均依据中华人民共和国的有关法律法规执行。
安徽CA只有在用户证书有效期限内承担这种损失或损害赔偿。

9.8.1.2 RA 承担责任的限制

RA 承担责任的限制在RA 与安徽CA之间签订的协议中表明。

9.8.1.3 受理点承担责任的限制

受理点承担责任的限制在受理点与安徽CA之间签订的协议中表明。

9.8.2 索赔

由以下情况造成用户或依赖方的损失并同时损害安徽CA利益的，安徽CA拥有向用户和依赖方索取赔偿的权利。这些情况是：

① 用户没有提供正确的身份信息而申请到信息不正确的证书的；

② 用户在证书应用时不检查证书吊销信息CRL 的；

③ 用户未按规定使用证书，有意或无意泄漏证书相关私密信息的；

④ 将证书应用于安徽CA不允许的领域或应用的；

⑤ 其它不符合安徽CA要求和规定的行为。

9.9 CPS 的有效期与终止

安徽CA的CPS 自发布之日起正式生效。CPS 中将详细注明版本号及发布日期。最新版本的CPS 请访问安徽CA网站以获得，对具体个人不做另行通知。当新版本的CPS 正式发布生效，则旧版本的CPS 将自动终止。

9.10 CPS 的修订

当出现以下情形时。安徽CA将对CPS 进行修订：

① 因相关法律法规要求而引起安徽CA业务规则发生改变。

② 因相关技术条件变化而引起安徽CA业务规则发生改变。

③ 因其它原因而引起安徽CA业务规则发生改变。

CPS 的修正的流程为：

① CPS 修订小组提出修订意见，征询各方的建议，包括用户和依赖方；

② 搜集各方意见并进行研究讨论；

③ 在CPS 修订小组进行修改并公司决策层批准；

④ 再次进行审议和生效，并通过公司网站或其它方式发布。

9.11 争议解决

当安徽CA与用户或依赖方出现争议，如通过协商仍未能达成一致意见时，当事人有权将争议提交当地仲裁机构，根据仲裁条例在时效内裁决。

9.12 管辖法律

安徽CA的电子认证业务规则（CPS）及协议中条款的制定均依从《中华人民共和国合同法》、《中华人民共和国电子签名法》以及中华人民共和国相关法律。

9.13 与适用法律的符合性

安徽CA的各项策略的执行、解释、翻译、和有效性均适用中华人民共和国法律法规和国家信息安全主管部门要求。法律的选择是确保对所有用户有统一的程序和解释，而不论他们在何地居住以及在何处使用证书。

9.14 一般条款

9.14.1 完整协议

现行条款替代所有以前的和同时期的条款。

9.14.2 分割性

对于法庭或其他仲裁机构判定某条款非法和不可执行而导致协议无法执行的情况，保留采用法律解决的权利。

9.14.3 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。

9.14.4 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。例如战争、恐怖行动、罢工、自然灾害、供货商或代理商倒闭、互联网或其它基础设施无法使用等。但各方都有义务建立灾难恢复和业务连续性机制。

9.15 各种规范的冲突

若本电子认证业务规则与其它规定、指导方针相互抵触，用户必须接受本电子认证业务规则的约束，除非本电子认证业务规则的规定在法律禁止的范围之

内，或有关规定、指导方针明确地言明优于本电子认证业务规则。

在安徽CA与包括用户在内的其它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，均视为双方均同意按本电子认证业务规则的规定执行；对协议中不同于本电子认证业务规则内容的约定，按双方协议中约定的内容执行。

9.16 补充说明

暂无。