HUNCA CPS

电子认证业务规则

版本**V4.4**

生效日期：**2019** 年**9**月**20**日

HUNCA CPS

Certification Practice Statement

Version 4.4

Effective Date：**Sep 20, 2019**

湖南 CA 电子认证业务规则
湖南省数字认证服务中心有限公司版权所有

版权声明

本规则的最新版本请参见本公司网页http://www.hunca.com.cn,或者联系湖南省数字认证服务中心有限公司。

地址： 湖南省长沙市岳麓区潇湘南路一段368号中盈广场C座13楼

邮编： 410006

电话：0731-88590261

传真：0731-88590262

电子邮件：service@hunca.com.cn

本规则如有改动，对特定对象不再另行通知。

注意：

《湖南 CA 电子认证业务规则》服从于中国的法律法规，包括且不限于：《中华人民共和国刑法》、《中华人民共和国人大常委会颁发的关于互联网安全防护措施的决定》、《中华人民共和国计算机安全管理条例》、《中华人民共和国商用密码管理条例》、《电子认证服务密码管理办法》、《中华人民共和国电子签名法》、《电子认证服务管理办法》。

对任何已经或即将涉嫌犯罪而影响湖南 CA 证书服务的组织、单位和个人，湖南 CA 将保留依法追诉的权利。

目 录

1 概括性描述

1.1 概述

1.1.1 湖南 CA

湖南省数字认证服务中心有限公司(Hunan Certification Authority Service Center Co.,Ltd，简称湖南 CA)于 2008 年开始运营，是权威、公正的电子认证服务机构。其宗旨是保证通过互联网络提供服务和享受服务的客户实现安全交易，为互联网络的客户提供网上身份认证和信任服务。

湖南 CA 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，以及其他相关管理规定，提供数字证书申请、颁发、存档、查询、废止等服务，并提供以 PKI 技术、数字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。

为了配合证书业务的正常开展，湖南 CA 建立了《湖南 CA 电子认证业务规则》，本电子认证业务规则的建立和实施，将为湖南省电子政务、电子商务和其他网上安全服务提供强有力的支持和保障。

湖南 CA 获取了主管单位中华人民共和国工业和信息化部颁发的《电子认证服务许可证》及国家密码管理局颁发的《电子认证服务密码使用许可证》等资质，并处于有效期内。

1.1.2 电子认证业务规则

湖南 CA、湖南 CA 授权的注册机构、注册分支机构、受理点、湖南 CA 授权或协议的单位等实体，统称为湖南 CA 认证体系内的实体或湖南 CA 关联实体。湖南 CA 认证体系内的实体和湖南 CA 数字证书持有者，必须完整地理解和执行《湖南 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。

《湖南 CA 电子认证业务规则》详细阐述了湖南 CA 实际工作和运行应遵循的各项规范。它支持多种湖南 CA 制定的证书策略。证书策略是证书管理、证书应用、证书分类、证书授权、证书责任等政策规则的集合。

电子认证业务规则作为实际应用和操作的文件依据，适用于湖南 CA、湖南 CA 授权机构、湖南 CA 数字证书签约单位、湖南 CA 实体内部员工、申请证书的单位和个人。作为公告，向社会公布湖南 CA 关于证书服务的基本立场和观点。在证书有效期内为证书申请者提供相关的咨询服务。湖南 CA 认证体系中涉及的单位和个人，必须完整理解和准确解释《湖南 CA 电子认证业务规则》的内容。

1.2 文档名称与标识符

1.2.1 名称

本文档名称为《湖南 CA 电子认证业务规则(HUNCA CPS)》，是湖南 CA 对所提供的认证及相关业务的全面描述。

1.2.2 版本

版本号 4.4。

1.2.3 发布

本文档将通过湖南 CA 公司网站（www.hunca.com.cn）面向社会公开发布。如有更新，将在湖南 CA 公司网站提供最新版本。

1.2.4 湖南 CA 标识

湖南 CA 公司是湖南省数字认证服务中心有限公司（Hunan Certification Authority Service Centre co.,ltd）的缩写形式。

湖南 CA 公司所拥有的品牌商标为：

1.3 电子认证活动参与者及其职责

1.3.1 电子认证服务机构

湖南 CA 是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定，依法设立的第三方电子认证服务机构。电子认证服务机构是

受用户信任，负责创建和分配公钥的权威机构，是颁发数字证书的实体。湖南 CA 通过给从事电子交易活动的各方主体颁发数字证书、提供证书验证服务等手段而成为电子认证活动的参与主体。

1.3.2 注册机构

注册机构作为电子认证服务机构授权委托的下属机构，包括注册系统（RA），和证书受理点（LRA），负责订户证书的申请、审批和管理；一般情况下 LRA 证书受理点进行用户身份鉴定和证书信息录入，提交到 RA 系统把证书申请信息传递到 CA。

湖南 CA 本身也承担 RA 职责，订户可以直接向湖南 CA 提出证书申请，除此之外湖南 CA 授权的合作机构，可以成为湖南 CA 的注册机构，承担本 CPS 中的注册机构的义务。

1.3.3 订户

在电子签名应用中，订户即是电子签名人，是接收 CA 机构签发证书的实体。

湖南 CA 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，以及其他持有湖南 CA 证书的人、物、对象或单位组织。

1.3.4 依赖方

在湖南 CA 证书服务体系中，依赖方是信任 CA 机构证书，可以对使用

CA机构证书机制进行的数字签名进行验证,使用CA机构证书的公钥的实体。依赖方包括个人、单位、服务器、网站等提供网上服务和享受网上服务的各种实体，以及其他持有湖南CA各类证书的人、物或组织单位。

作为湖南CA证书订户的依赖方,享有湖南CA提供的各种相应的权利,包括湖南CA可能提供的证书保障，以及本CPS中规定的权益。非证书订户的依赖方，湖南CA除了担保其所信任的并由湖南CA签发的证书和相关签名信息的真实性以外，不承担其他义务和责任。

1.3.5 其他参与者

其他参与者是指为湖南CA的电子认证活动提供相关服务的其他实体。

湖南CA电子认证活动的其他参与者包括以上未提及的，属于湖南CA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

湖南CA数字证书可以用于涉及身份识别、信息加密、行为确认的电子商务和电子政务应用，如工商、税务、质量监督、政府采购、海关、公共事业、金融服务业、检验检疫、车辆管理、政府行政办公、社保、保险、卫生等行业网上对外业务的开展以及各类电子交易和企事业单位内部办公等。按照证书的功能及使用证书的实体不同，湖南CA提供以下所列的多种证书。

证书种类	应用范围
个人证书	个人在网上活动中表明身份
机构证书	组织机构在网上活动中表明身份
设备证书	用于标识各种设备，实现设备标识以及交互数据的加解密功能，保证传输数据的完整性、安全性等
代码签名证书	对代码拥有者的身份进行标识，用于代码发行中的签名，以保护代码的完整性和安全性
云移动证书	用于证明用户在移动化和云服务环境中所进行的身份认证和电子签名

1.4.2 限制的证书应用

湖南 CA 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订户负责。

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 的管理机构为湖南 CA 安全策略管理委员会。由湖南 CA 安全策略委员会负责本 CPS 的编写、修订和发布事宜。

1.5.2 联系人

湖南CA 对电子认证业务规则进行严格的版本控制，并由湖南CA公司负责解释。

电话：0731-88590261

传真：0731-88590262

邮编：410006

地址：湖南省长沙市岳麓区潇湘南路一段368号中盈广场C座13楼

电子邮件：service@hunca.com.cn

1.5.3 决定 CPS 符合策略的机构

湖南 CA 公司的安全策略管理委员会拥有对湖南 CA CPS 的决策权和审批权。

1.5.4 电子认证业务规则批准程序

湖南 CA 的 CPS 由安全策略管理委员会指定的“CPS 编写小组”起草拟定后，提交安全策略管理委员会审核。如需进行变更，由“CPS 编写小组”提交变更报告并进行修改，安全策略管理委员会对提供的变动建议进行研究分析，形成最终决议。湖南 CA 公司将在决议形成后，在网站公布变更后的《湖南 CA 电子认证业务规则》正式文档。每次修订完成后均需由湖南 CA 公司的安全策略管理委员会审批，自发布之日起 30 日内向行业主管部门报备。

1.5.5 公告

所有公告和通知将在湖南 CA 网站上公布。

1.6 定义与缩写

1.6.1 电子认证服务机构

受用户信任，负责创建和分配公钥证书的权威机构。

1.6.2 注册机构

CA 的注册机构（Registration Authority），简称 RA。是湖南 CA 设立的数字证书业务受理机构或与湖南 CA 签署注册机构协议，由湖南 CA 授权发行湖南 CA 证书的代理机构。注册机构负责执行湖南 CA 的证书管理策略，负责证书申请者证书申请信息的收集和审核以及证书的发放等工作。

1.6.3 运营安全策略管理委员会

由湖南 CA 任命的负责湖南 CA 运营策略和规范的开发、维护以及湖南 CA 安全策略的制定和监督执行的组织。

1.6.4 对象标识符

缩写为 OID，是一个属性，通常是一个编号，用来唯一标识一个对象。

1.6.5 订户

订户（Subscribers）指由湖南 CA 签发的各类证书的持有者，也被称为客户或者用户。

1.6.6 依赖方

依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的个人或机构。

1.6.7 甄别名

甄别名（Distinguished Name）简称 DN，包含订户的属性信息，具有唯一性。

1.6.8 KMC

密钥管理中心简称 KMC，负责密钥的产生、存储、归档等管理工作。

1.6.9 OCSP

OCSP（Online Certificate Status Protocol），即在线查询数字证书状态协议，用于支持实时查询数字证书状态信息。

1.6.10 LDAP

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）。

1.6.11 PKI

PKI（Public Key Infrastructure），公共密钥基础设施。

支持公开密钥体制的安全基础设施，提供身份鉴别、加密、完整性和

不可否认性服务。

1.6.12 CRL

CRL（Certificate Revocation List），即数字证书废止列表的英文简称。CRL 中记录所有在原定失效日期到达之前被废止的数字证书的订户数字证书序列号，供数字证书使用者在认证对方数字证书时查询使用。CRL 通常又被称为数字证书黑名单。内容通常还包含 CA 机构的名称、发行日期、下次废止列表的预定发行日期、更新或废止的数字证书序列号，并说明更新或废止的时间与理由。

1.6.13 ARL

CA 注销列表（Certificate Authority Revocation list），一个经电子认证服务机构数字签名的列表，标记已经被注销的 CA 的公钥证书列表，表示这些证书已经无效。

1.6.14 认证

认证（Certification）指不同实体在进行网上交易之前，通过可信赖的、中立的第三方（如湖南 CA）对身份进行审核，并由第三方出具证明证实其身份的可靠性和合法性的过程。

1.6.15 电子签名

电子签名，是利用公开密钥算法等方法保证信息传输过程中信息的完

整性和提供信息发送者的身份认证及不可抵赖性的一种技术。

1.6.16 私有密钥

私有密钥（Private Key），是一种不能公开、由持有者秘密保管的数字密钥，用于创建电子签名、解密报文或与相应的公开密钥一起加密文件。

1.6.17 公开密钥

公开密钥（Public Key），是可以公开的数字密钥，用于验证相应的私有密钥签名的报文，也可以用来加密报文、文件，由相应的私有密钥解密。

1.6.18 签名密钥对

证书申请者申请证书时由客户端产生。主要用于订户的签名和验证，包含一对密钥，即私有签名密钥和公开签名密钥。

1.6.19 加密密钥对

证书申请者申请证书时由 KMC 产生。主要用于订户信息的加解密，包含一对密钥，即私有加密密钥和公开加密密钥。

2 信息发布与信息管理

2.1 认证信息的发布

湖南CA通过目录服务（LDAP）发布证书状态的相关信息，订户可以通过访问湖南CA 的目录服务器获取证书的信息。湖南CA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。

湖南CA 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。湖南CA 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验证证书有效性。

湖南CA 证书订户都可以通过湖南CA 网站（www.hunca.com.cn）查询有关信息。

2.2 证书的发布时间及频率

湖南 CA 目录服务器上每日更新目录，可以实时和定时发布，通常在 24 小时内自动发布最新 CRL。

2.3 信息库访问控制

2.3.1 信息的发布与处理

湖南 CA 对外发布 CPS、证书、CRL、证书服务协议等公开信息，允许公众自行通过网站和目录服务器进行查询和访问。湖南 CA 将及时在网站上公布新的信息。

2.3.2 信息访问控制

湖南 CA 设置了信息访问控制和安全审计措施，保证只有经过授权的湖南 CA 工作人员才能编写和修改湖南 CA 在线的公告和公布信息，但不限制对这些信息的阅读权。湖南 CA 在必要时可自主选择是否实行信息的权限管理，以确保湖南 CA 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

湖南CA颁发的证书，含订户证书主体甄别名（Distinguished Name，简称 DN）,唯一标识证书订户的身份。命名符合X.500 甄别名规定。

3.1.2 名称形式遵守的规则

湖南 CA 证书符合 X509.3 标准，甄别名格式遵守 X.500 标准。格式如下：

属性	值	举例
Country（C） =	国家	CN
Organization（O） =	组织	湖南 CA
Organizational Unit （OU） =	组织机构	技术部
State or Province （S） =	省	湖南省
Locality （L） =	市	长沙市
Common Name （CN） =	通用名	张三

3.1.3 对名称意义化的要求

订户的甄别名(DN)必须具有一定的代表意义。

证书主体名称标识本证书所提到的最终实体的特定名称，描述了与主

体公钥中的公钥绑定的实体信息。

3.1.4 订户的匿名或伪名

湖南 CA 证书服务体系中，订户（证书申请人）不宜使用匿名或伪名。

3.1.5 理解不同名称形式的规则

依 X.501 甄别名命名规则解释。

3.1.6 名称的唯一性

名称对湖南 CA 的所有证书持有者，要求必须是唯一的。湖南 CA 根据该名称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。对于同一订户，可以用主体名为其签发多张证书，但证书的扩展项不同。

3.1.7 商标的识别、鉴别和角色

湖南 CA 签发的证书中不包含任何商标名。

3.2 初始身份验证

3.2.1 证明持有私钥的方法

通过证书请求中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。

在湖南 CA 证书服务体系中，订户签名私钥在订户端生成，订户证书请

求信息中包含用私钥进行的数字签名，湖南 CA 用其对应的公钥来验证这个签名。证书申请人被视作其签名私钥的唯一持有者，因此湖南 CA 要求证书申请人妥善保管自己的签名私钥。

云移动证书服务体系中，私钥在订户终端和云端共同计算生产，证书请求信息中包含用私钥进行的数字签名，订户移动终端和云端共同计算生产的公钥来验证这个签名，视作申请人为其私钥的拥有者。

3.2.2 组织机构身份的鉴别

对于组织身份的鉴别，湖南 CA 需要验证组织的合法证件。证书申请人需持工商营业执照、全国组织机构代码证书或统一社会信用代码登记证书等证件，以及组织给经办人的授权文件和经办人身份证件，向 CA 机构提出申请。

湖南 CA 保留根据最新国家政策法规的要求更新组织身份鉴别规范的权利。更新后的组织身份鉴别要求将发布在湖南 CA 的网站上：http://www.hunca.com.cn/

经办人经组织授权，并携带授权文件及本人身份证的原件和复印件，到湖南 CA 授权的注册机构提交书面数字证书申请表（一式三份）及下述组织证明文件等申请资料，并缴纳证书服务费用。

1、 组织机构代码证的副本及复印件

2、 工商营业执照副本及复印件，如果组织没有营业执照，则可选其他有效证书的副本及复印件，部分有效证件如下：

- 企业法人营业执照

- 事业单位法人登记证
- 事业单位登记证
- 社会团体登记证
- 地税税务登记证
- 政府批文
- 其他有效证件

3、 经办人有效身份证件的原件和复印件

注：已办“三证合一”的组织只需提交加载统一社会信用代码的证件和上述资料中的第三点资料。

以上证明文件的复印件需加盖申请单位的公章。

湖南 CA 授权的注册机构按照湖南 CA 组织身份鉴别要求对申请资料的原件和复印件真实性进行审核，并进行批准申请或拒绝操作。批准申请后，湖南 CA 或注册机构将保留相关盖单位公章的证明材料复印件，与证书申请表一并存档保存。

3.2.3 个人身份的鉴别

个人身份的鉴别可以使用以下有效的身份证件：居民身份证、港澳台居民身份证、户口簿、护照、外国人永久居留证。

湖南 CA 保留根据最新国家政策法规的要求更新个人身份鉴别规范的权利。更新后的个人身份鉴别要求将发布在湖南 CA 的网站上：http://www.hunca.com.cn/

个人需持上述个人有效身份证件，到湖南CA授权的注册机构提交书面

数字证书申请表（一式三份）和上述有效身份证件的复印件等申请资料，并缴纳证书服务费用。

湖南CA授权的注册机构按照湖南CA个人身份鉴别要求对申请资料的原件和复印件真实性进行审核，并进行批准申请或拒绝申请的操作。批准申请后，湖南CA或注册机构将保留复印件，与证书申请表一并存档保存。

3.2.4 域名（或 IP 地址）的确认和鉴别

如果设备证书的关键项为域名（或IP地址），除了在对申请者递交的书面材料进行审核外，湖南CA需要申请者提供额外的域名（或IP地址）使用权证明材料，或向相应的域名注册服务机构（IP注册服务机构）或者其他第三方查询，以确定申请者是否有权使用相应的域名（或IP地址）。湖南CA还需要采取其他独立的审查措施，以确认该域名（或IP地址）的归属权，如果要求申请者提供相应的协助，该申请者不得拒绝这种请求。当由于域名（或IP地址）的归属问题发生证书签发纠纷时，湖南CA保留根据该域名（或IP地址）的实际归属情况签发或废除设备证书的权利。

3.2.5 云移动证书订户身份的鉴别

云移动证书订户的身份鉴别参照个人和组织机构身份方法进行鉴别。

云移动证书身份鉴别也可以通过适当的在线的方式来进行鉴别。订户可以通过手机拍照、证件照上传等方式提交材料。湖南CA或注册机构可通过人脸生物识别技术及可信数据源验证订户的身份信息进行身份鉴别审核。

3.2.6 没有验证的订户信息

没有验证过的信息包括但不限于电话号码、邮编、地址、电子邮件等，湖南 CA 将对这些信息采取保密措施，但不承担由于该信息引起的任何责任和纠纷。

3.2.7 授权确认

为组织机构的人员或设备办理证书申请的人，需要出具该组织机构授权其为该机构办理湖南 CA 数字证书事宜的授权文件。

组织在湖南 CA 的数字证书申请授权委托书上加盖单位公章后，则证明本组织对办理人的授权确认。

3.2.8 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。但交叉认证并不表示湖南 CA 批准了或赋予了其他 CA 中心或电子认证服务机构的权力。

3.3 密钥更新请求的标识与鉴别

通常，订户的密钥存在有效期，湖南CA 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。

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，湖南 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

吊销后密钥更新中对身份标识和鉴别的要求，使用与原始身份验证相同的流程，参见 3.2 初始身份确认。

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，参见 3.2 初始身份确认。

如果是因为订户没有履行本《电子认证业务规则》所规定的义务，由注册机构申请吊销订户的证书时，不需要对订户身份进行标识和鉴别。

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

证书申请实体包含个人、企业单位、事业单位、政府机构、社会团体等各类组织机构。任何合法的组织和个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。

4.1.2 注册过程与责任

证书申请人按照本电子认证服务规则所规定的要求，填写证书申请表，并准备相关的身份证明材料。湖南 CA 或注册机构依据身份鉴别规范对证书申请人的身份进行鉴别，并决定是否受理申请。

申请过程中各方责任为：订户要按照本电子认证服务规则 3.2 所述的要求准备证书申请材料，并确保申请材料真实准确。

湖南 CA 及注册机构负责接收证书申请人的证书申请材料，对订户所提供的证书申请信息与身份证明资料的一致性进行查验。

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

湖南 CA 数字证书申请流程为：

1. 证书申请应由证书申请人或相应的授权人提交，申请者可以从湖南 CA 的网站下载或到湖南 CA 授权的注册机构领取相应的证书申请表，按表格要求填写申请表；或通过湖南 CA 的在线服务系统提交申请信息。

2. 按照本文 3.2 身份鉴别要求提交对应的证书申请表格及相关身份证明材料，到湖南 CA 或授权的注册机构进行注册、身份审核和缴费。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

湖南 CA 或授权的注册机构按照本《电子认证业务规则》所规定的身份鉴别流程对申请人的身份进行识别与鉴别。具体的鉴别流程详见§3.2 初始身份验证。

4.2.2 证书申请的批准和拒绝

湖南 CA 根据本《电子认证业务规则》所规定的身份鉴别流程对证书申请人身份进行识别与鉴别后，根据鉴别结果决定接受或拒绝证书申请。

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

证书申请人未能通过身份鉴证，湖南 CA 或注册机构将拒绝申请人的证书申请，并通知申请人鉴证失败，同时向申请人提供失败的原因(法律禁止的除外)。被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

4.2.3 处理证书申请的时间

湖南 CA 授权的注册机构必须确保快速处理证书申请信息，一旦注册机构收到了证书申请所有必须的相关资料，湖南 CA 将在接受用户申请 2 个工作日内对证书申请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 证书签发过程中电子认证服务机构的行为

湖南 CA 在接受证书申请并审核通过之后，将签发证书。证书的签发意味着电子认证服务机构最终完全正式地受理了证书申请。证书从订户接受证书那天起将被视为有效证书。

4.3.2 电子认证服务机构对订户的通告

电子认证服务机构通过注册机构，对订户的通告有以下几种方式：

- 通过面对面的方式，通知订户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订户；
- 邮政信函等通知订户；
- 其他湖南 CA 认为安全可行的方式通知订户。

4.4 证书接受

4.4.1 构成接受证书的行为

证书申请用户可以在向湖南 CA 成功提交证书申请后，凭证书申请表领取证书，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，应妥善保存其证书对应的私有密钥和承载证书的介质。

湖南 CA 签发的云移动证书，订户所使用移动设备或 APP 应用程序接收到数字证书起，被视为同意接收证书。

4.4.2 电子认证服务机构对证书的发布

湖南 CA 在签发完证书后，就将证书发布到数据库和目录服务器中。湖南 CA 采用主、从目录服务器结构来发布所签发证书。签发完成的数据直接写入主目录服务器中，然后通过主从映射，将主目录服务器的数据自动发布到从目录服务器中，供订户和依赖方查询和下载。

湖南 CA 签发的云移动证书，会将证书信息进行保存，订户移动终端会对证书状态实时监测。根据依赖方约定，可向依赖方提供状态查询服务。

4.4.3 电子认证服务机构对其他实体的通告

其他实体可以通过从目录服务器中查询到湖南 CA 已经签发的数字证书。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户使用证书时，必须妥善保管和存储与证书相关的私钥，避免遗失、泄露、被篡改或者被盗用。任何人使用证书都必须检验证书的有效性，证书到期或吊销后，须停止使用该证书及对应的私钥，如果证书持有人继续使用该证书，湖南 CA 将不承担任何由此产生的责任和义务。

在使用与湖南 CA 所签发的证书有关的签名及经过签名的信息时，参与方（湖南 CA、证书订户和依赖方等）按本 CPS 的规定享有相应的权利和应尽的义务。参与方均视为已被通知并同意遵守本 CPS 以及湖南 CA 与各方

签署的协议、规范中的条款。任何超出本 CPS 的规定的证书及私钥的使用，湖南 CA 将不承担由此带来的任何后果。

湖南 CA 签发的各类证书，仅用于表明证书持有者在申请证书时所要标识的身份，以及验证证书持有者用于该证书包含的公钥相对应的私钥做出的签名。这样，通过签名和签名的验证，保证证书持有者的身份真实性、信息的完整性、信息的不可抵赖性等。如果证书持有人将该证书用于其它用途，湖南 CA 将不承担任何由此产生的责任和义务。

如果证书中的某些字段明确了证书的使用范围和用途，那么该证书将只被允许在这一范围内使用。任何超出证书所标明的适用范围内的行为，都将由行为人独立承担责任。湖南 CA 对超出适用范围内的任何使用行为，不承担任何由此产生的责任和义务。

4.5.2 依赖方对公钥和证书的使用

依赖方有义务妥善保存订户的公钥和证书，不将其用于不适合的证书用途，使用前有责任检查证书的真实性和有效性。

在信任证书和签名前，依赖方要独立地作出应有的努力和合理的判断。除非本 CPS 另有规定，证书并不是来自发证机构的对任何权利或特权的承诺。依赖方在本 CPS 规定的范围内信赖证书和证书中包含的公钥，并对此做出决定。如果证书中的某些字段明确了证书的使用范围和用途，那么该证书将只被允许在这一范围内进行使用。依赖方必须对此做出合理的判断，任何对超出证书所标明的适用范围的行为的信赖，都将由依赖方独立承担责任，湖南 CA 对此不承担任何责任和义务。

验证证书的有效性包括三个方面的内容：

- 用湖南 CA 的证书验证证书中的签名，确认该证书是由湖南 CA 签发的，并且证书的内容没有被篡改。
- 检验证书的有效期，确认该证书在有效期之内。
- 查询证书状态，确认该证书没有被注销。

在验证电子签名时，依赖方应准确知道什么数据已被签名。在公钥密码标准里，用标准的签名信息格式来准确表示签名过的数据。

4.6 证书更新

4.6.1 证书更新的情形

证书更新是指在不改变订户证书中的公钥或证书中任何订户信息不变的情况下，为订户签发一张新证书。在证书上都有明确的证书有效期，表明该证书的起始日期与截至日期。订户应当在证书有效期到期前，到湖南 CA 授权的注册机构申请更新证书。

证书更新由订户自行决定采用证书更新或证书密钥更新。

4.6.2 请求证书更新的实体

订户可以申请证书更新。订户包括湖南 CA 签发的各类证书的证书持有人。

4.6.3 证书更新请求的处理

- 申请者用面对面或者在线的方式向湖南 CA 提交证书更新申请，并

注明更新的原因。

- 湖南 CA 或授权的注册机构按照（§3 章节）身份标识与鉴别办法对订户提交的证书更新申请进行审核。审核通过后，为订户完成证书更新。

4.6.4 颁发新证书时对订户的通告

同§4.3.2 节。

4.6.5 构成接受更新证书的行为

同§4.4.1 节。

4.6.6 电子认证服务机构对更新证书的发布

同§4.4.2 节。

4.6.7 电子认证服务机构在颁发证书时对其他实体的通告

同§4.4.3 节。

4.7 证书密钥更新

证书密钥更新是指订户生成一对新密钥并申请为新公钥签发新证书。

4.7.1 证书密钥更新的情形

- 当订户证书即将到期或已经到期时；
- 当订户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；

- 当订户证实或怀疑其证书密钥不安全时；
- 其他可能导致密钥更新的情形。

4.7.2 请求证书密钥更新的实体

订户可以申请证书密钥更新。订户包括湖南 CA 签发的各类证书的证书持有人。

4.7.3 证书密钥更新请求的处理

- 申请者用面对面或者在线的方式向湖南 CA 提交证书密钥更新申请，并注明更新的原因。
- 湖南 CA 或授权的注册机构按照（§3 章节）身份标识与鉴别办法对订户提交的证书密钥更新申请进行审核。审核通过后，为订户完成证书密钥更新。
- 新证书签发后旧的证书将被注销（§4.10）。湖南 CA 将在 2 小时内在 LDAP 上发布订户的新证书。订户旧证书废止信息在 24 小时内通过 CRL 发布。

4.7.4 颁发新证书对订户的通告

同§4.3.2 节。

4.7.5 构成接受密钥更新证书的行为

同§4.4.1节。

4.7.6 电子认证服务机构对密钥更新证书的发布

同§4.4.2节。

4.7.7 电子认证服务机构在颁发证书时对其他实体的通告

同§4.4.3节。

4.8 证书变更

证书的变更是指证书订户的信息发生变化，在不改变现有公钥的情况下重新申请一张证书。湖南CA不提供证书变更业务，订户要变更证书中的内容时，视为申请一张新证书，且证书的申请及处理流程与申请新证书一致。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

- 新的密钥对替代旧的密钥对；
- 密钥失密：与证书中的公钥相对应的私有密钥被泄密或订户怀疑自己的密钥失密；
- 从属关系改变：与密钥相关的订户的主题信息改变，证书中的相关信息有所变更；

- 操作中止：由于证书不再需要用于原来的用途，但密钥并未失密，而要求中止（例如订户离开了某个组织）；
- 订户不能履行电子认证业务规则或其他协议、法律及法规所规定的责任和义务；
- 订户申请初始注册时，提供不真实材料；
- 证书已被盗用、冒用、伪造或者篡改；
- CA 失密：电子认证服务机构因运营问题，导致 CA 内部重要数据或 CA 根密钥失密等原因；
- 利用数字证书在网上进行违法犯罪活动的；
- 其他情况：这些情况可以是因法律或政策的要求湖南 CA 采取的临时注销措施，也可以是订户申请注销证书时填写的其他原因。

4.9.2 请求证书吊销的实体

已申请湖南 CA 证书的订户可以请求吊销证书；

湖南 CA 可在 4.9.1 章节所述的情形下主动吊销订户证书。

4.9.3 吊销请求的流程

- 申请者到湖南 CA 或授权的注册机构书面填写《湖南 CA 个人数字证书业务申请表》或《湖南 CA 单位数字证书业务申请表》，并注明吊销的原因。
- 湖南 CA 或授权的注册机构按照（§3 章节）身份标识与鉴别办法对订户提交的相关业务申请进行审核；

- 强制吊销：当吊销情形出现时，湖南 CA 或经湖南 CA 授权的注册机构可以对订户证书进行强制吊销，吊销后必须立即通知该证书订户。被吊销的订户证书在 24 小时内通过 CRL 向外界公布。

4.9.4 吊销请求宽限期

订户一旦发现需要吊销证书，应及时向湖南 CA 提出吊销请求。

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。其他吊销原因的吊销请求必须在 48 小时内提出。

4.9.5 电子认证服务机构处理吊销请求的时限

发证机构在接到订户挂失、废除、注销等数字证书吊销申请时，应及时受理。在受理后 24 小时内保证数字证书吊销操作正式生效。在订户办理数字证书吊销相关手续前及发证机构受理订户证书吊销相关申请时起到证书吊销生效时 24 小时内造成的损失，发证机构不承担相关法律责任。湖南 CA 每 24 小时签发一次 CRL，并将最新的 CRL 发布到目录服务器指定的位置，供请求者查询下载。

4.9.6 依赖方检查证书吊销的要求

依赖方需要访问湖南 CA 目录服务器或 OCSP 来查询订户的证书状态，以获得订户证书的状态信息。注意：依赖方要验证证书的可靠性和完整性，确保证书是经湖南 CA 发布并且签名的。

4.9.7 CRL 的发布频率

湖南 CA 可采用实时或定期的方式发布 CRL，订户可以访问 CRL 验证证书当前状态。颁发 CRL 的频率根据证书策略确定，一般为 24 小时定期发布。订户有特殊要求的，将根据订户的需求，适当更新 CRL 发布的频率。

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 在线状态查询的可用性

湖南 CA 提供 7X24 小时 LDAP 目录查询服务。并提供了 OCSP 作为可选的在线状态有偿查询方式。

4.9.10 在线状态查询要求

证书基本信息查询可对证书序列号、证书主题、证书状态、证书有效期进行查询。

证书附加信息查询可对证书所相对应的订户信息如订户名、电子邮件地址等进行查询。

4.9.11 吊销信息的其他发布形式

OCSP 作为可选的吊销信息发布形式。

4.9.12 密钥损害的特别要求

无论是订户还是湖南 CA、注册机构，发现其密钥遭受安全威胁时，应及时吊销证书。

4.9.13 证书挂起

湖南 CA 暂不提供证书挂起业务。

4.10 证书状态服务

4.10.1 操作特征

湖南 CA 通过目录服务器为订户提供证书状态服务。

4.10.2 服务可用性

湖南 CA 提供 7X24 小时的证书状态查询服务。

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：

- 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，订户可以终止订购；
- 在证书有效期内，证书被吊销后，即订购结束。

4.12 密钥生成、备份与恢复

订户的签名密钥对由订户的密码设备（如智能 USB-KEY 或智能 IC 卡）生成，加密密钥对由密钥管理中心生成。

签名密钥对由订户的密码设备保管。

密钥恢复是指加密密钥的恢复，密钥管理中心不负责签名密钥的恢复。密钥恢复分为两类：订户密钥恢复和司法取证密钥恢复。

- 订户密钥恢复：当订户的密钥损坏或丢失后，某些密文数据将无法还原，此时订户可申请密钥恢复。订户在湖南 CA 或授权的注册机构申请，经审核后，通过湖南 CA 向 KMC 请求；密钥恢复模块接受订户的恢复请求，恢复订户的密钥并下载于订户证书载体中。
- 司法取证密钥恢复：司法取证人员在 KMC 申请，经审核后，由密钥恢复模块恢复所需的密钥并记录于特定载体中。

  云移动证书的密钥对，由订户移动终端和云端协同计算产生。由终端和云端分别各自进行密钥备份与恢复。

5 认证机构设施、管理和操作控制

5.1 物理控制

湖南 CA 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湖南 CA 的运营设施和信息安全。防止未经过授权的物理访问确保未经过授权的人或仅被授权访问有限物理区域的人员不得访问湖南 CA 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

湖南CA主机房位于长沙市区。在湖南CA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，设置了可以控制进出的带锁的门来控制每个人进出每一个区域。每一层区域都有非常严格的控制方法防止未授权的物理访问。机房所有关键设施使用能够阻止和监测隐蔽性穿透的材料建造。敏感区域采用屏蔽机房建设，墙壁采用镀钢夹层加固；只使用一个足以抵制用力的进入的门作为敏感区域的常规入口。

湖南 CA 的建筑物和机房建设按照下列标准实施：

GB 2887-89《计算站场地技术条件》
GB 50174-93《电子计算机机房设计规范》
SJ/T30003-93《电子计算机机房施工验收规范》
GB 50016-2006《建筑设计防火规范》
GB 50222—95《建筑内部装修设计防火规范》
GB 9361-88《计算站场地安全要求》
GB 6650-86《计算机机房用活动地板技术条件》
GB 50116-2008《火灾自动报警系统设计规范》
GB 50057-2010《建筑物防雷设计规范》
GB 5054-2011《低压配电设计规范》
GBJ19-2003《采暖通风与空气调节设计规范》
YD\T754-95《通讯机房静电防护通则》
GB 8702-88《电磁辐射防护规则》
GB 12190《高性能屏蔽室屏蔽效能的测量方法》

5.1.2 物理访问

为了保证本系统的安全，采取了一定的隔离、控制、监控手段。机房的所有门都符合相关规定的安全性要求，能防止非法的进入。机房通过设置门禁和监控系统来重点实现机房物理安全。

物理访问控制包括如下几个方面：

- 门禁系统：控制各层门的进出权限。授权工作人员需使用身份识别卡结合指纹识别后才能进出，进出每一道门应有时间纪录。
- 报警系统：当发生任何非法闯入、非正常手段的开门、长时间不关门等异常情况都能触发报警系统。
- 监控系统：与门禁系统配合使用的还有录像监控系统，对安全区域和操作区域进行 24 小时不间断录像。

门禁和监控系统备有UPS电源，并提供至少8小时的不间断供电。

5.1.3 电力与空调

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统，按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备独立供电。供配电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。

使用不间断电源（UPS）来保证供电的稳定性和可靠性。采用双电源，在单路电源中断时，可以切换另一条线路，维持系统正常运转。

湖南CA的机房使用精密空调，并采用独立空调作为备份，根据GB50174-93《电子计算机机房设计规范》的有关规定，保证机房内温湿度达到国家标准。

5.1.4 水患防治

湖南CA有专门的技术措施防止、检测漏水的出现，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

湖南CA机房采用防火材料建设，安装有火灾自动报警系统和自动灭火消防系统，并通过国家权威部门的消防功能验收。系统通过设置在机房的温感和烟感采集消防数据，提供系统实时处理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

系统实时监测和系统的手动、自动控制模式的设定，并完成系统设计的各种联动动作。

5.1.6 介质存储

存储介质必须得到安全可靠的保护，避免诸如温度、湿度和磁力等环境变化可能产生的危害和破坏。

5.1.7 设备、资料报废处理

当湖南CA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，湖南CA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

湖南CA 对关键数据及其它敏感信息进行备份，这些备份信息保存在湖南CA 机房以外的安全建筑物地方。

5.2 程序控制

5.2.1 可信角色

电子认证服务机构、注册机构、依赖方等组织中与密钥和证书生命周期管理操作有关的工作人员，包括客户服务人员 、安全管理人员、密钥与密码设备管理人员、系统管理人员、人力资源管理人员等可信角色，必须由可信人员担任。

5.2.2 每项任务需要的人数

湖南CA确保单个人不能接触、导出、恢复、更新、废止湖南CA系统所存储的根证书对应的私有密钥。

至少有两个人以上共同实施，才能进行任何密匙恢复操作。

湖南CA对与运行和操作相关的职能有明确的分工，贯彻职责分割、多人控制、互相牵制和最小权益的安全管理原则。

5.2.3 每个角色的识别与鉴别

所有湖南CA的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡和指纹识别；进入系统需要使用数字证书进行身份鉴别。湖南CA将独立完整地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、操作和管理分离的原则，湖南

CA的可信角色由不同的人员担任。要求职责分割的角色包括（但不限于）以下几种：

- 密钥管理员
- 审计员
- 系统管理员
- 网络管理员
- 录入员
- 审核员

5.3 人员控制

5.3.1 资格、经历和无过失要求

湖南CA所有的员工必须与湖南CA签定保密协议。对于充当可信角色或其他重要角色的人员，必须具备的一定的资格。湖南CA确立流程管理规则，据此湖南CA员工将受到国家法律法规、劳动合同和湖南CA中心相关规章制度的约束，不得泄露湖南CA证书服务体系的敏感信息。

湖南 CA 要求充当可信角色的人员至少必须具备忠诚、可信赖及工作的热诚度、无影响 CA 运行的其它兼职工作、无同行业重大错误记录等。

一般情况下，人力资源部及用人部门共同负责对湖南 CA 可信任员工的背景、资历及经验进行真实性核实。如有必要，湖南 CA 将与本地有关的政府部门和调查机构合作，完成对湖南 CA 可信任员工的背景调查。

5.3.2 背景审查程序

湖南 CA 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。对于员工的考核周期一般为 3 个月，据考察的结果安排相应的工作或者予以辞退。湖南 CA 根据需要不定期对员工进行职责、岗位、技术、政策、法律、安全等方面的培训。

湖南 CA 会对其关键的职员进行严格的背景调查。注册机构、注册分支机构和受理点操作员的审查可以参照湖南 CA 对可信任员工的考察方式。受理点责任单位可以在此基础上，增加考察和培训条款，但不得违背湖南 CA 证书受理的规程和《湖南 CA 电子认证业务规则》。

湖南 CA 在开始一个可信任角色雇佣关系前会依据以下流程对其进行审查：

（1）应聘者应提交的个人资料：履历、最高学历证书、学位证书、户籍本或身份证、资格证、离职证明等相关有效证明。

（2）应聘者个人身份的确认：人力资源部通过电话、信函、网络、走访、调阅档案等形式对其提供材料的真实性进行鉴定。

（3）三个月的试用期考核：用人部门通过技术考核、日常观察、情景考验等方式对其进行考察。

（4）经考核，人力资源部和用人部门联合填写《拟录用人员背景调查表》，报主管领导批准后准予上岗。

5.3.3 培训要求

湖南 CA 对录用人员按照其岗位和角色安排培训，培训内容主要有：公司简介、内部规章制度、岗位职责、产品知识、系统硬件安装与维护、系统软件运行与维护、密码技术、PKI 体系结构、CA 和 KMC 系统安全管理以及系统的备份与恢复、CA 中心的运行管理、证书的生成、签发和管理以及产品质量控制体系、机房消防、门禁和监控系统安全管理、《湖南 CA 电子认证业务规则》（CPS）、湖南 CA 内部管理制度、政策、规定、标准和程序等。

5.3.4 再培训周期和要求

湖南 CA 每年至少向员工提供一次业务培训机会以不断提高其职业技能，以保证其完成工作所需要的职业水平。同时，根据策略调整、技术进步、系统功能更新或新系统的加入等情况，湖南 CA 也会对员工进行相应的培训，以适应新的变化。

5.3.5 工作岗位轮换周期和顺序

对于可替换角色，湖南 CA 将根据业务的安排进行工作轮换。轮换的周期和顺序，视业务的具体情况而定。

5.3.6 未授权行为的处罚

当湖南 CA 员工进行了未授权或越权操作，湖南 CA 在确认后立即作废或终止该人员的安全令牌和相关证书，中止该员工进入湖南 CA 证书服务

体系。根据情节严重程度，实施包括辞退或提请司法机关处理等措施。因未授权或越权操作给湖南 CA 中心或订户造成损失的，当事人负有赔偿责任。

5.3.7 独立合约人的要求

对不属于湖南 CA 内部的工作人员，但从事湖南 CA 有关业务的人员等独立签约者(如注册机构的工作人员)，湖南 CA 的统一要求如下：

a) 人员档案进行备案管理；

b) 具有相关业务的工作经验；

c) 必须接受湖南 CA 组织的岗前培训；

d) 需签署保密协议。

5.3.8 提供给员工的文档

为使得系统正常运行，湖南 CA 向其员工提供完成其工作所必须的文档。

5.4 审计日志程序

5.4.1 记录事件的类型

湖南 CA 的 CA 和 RA 运行系统，记录所有与物理环境安全、网络安全、密码和令牌安全、证书处理系统应用与数据安全、人员操作行为、操作系统和数据库运行安全等相关事件，以备审查。这些记录，无论是自动生成的还是手写、书面、电子文档或录像形式，都包含事件日期、事件的内容、

事件的发生时间段、事件相关的实体等。湖南 CA 还将记录其它认为有必要做记录的事件，例如：机房参观记录、人事变动等。

5.4.2 处理日志的周期

湖南 CA 将每季度对记录进行审查，将审查内容和结果备案。

5.4.3 审计日志的保存期限

湖南 CA 在数据库保存审计日志至少半年，离线存档保存期为至少五年。

5.4.4 审计日志的保护

湖南 CA 授权的人员才能对审计日志进行相应操作。审计日志处于严格保护状态，严禁未经授权的任何操作。

5.4.5 审计日志备份程序

湖南 CA 保证所有的审计记录和审计总结都按照湖南 CA 数据和资料备份管理的有关要求和程序进行。根据数据重要性、性质和要求，采用在线和离线相结合的备份形式。

日常备份采用每月手工在硬盘上保存备份数据压缩包的方式。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，通常以季度或者半年为时间单位的备份。操作上采用手工在光盘上备份数据的方式。此外，在对系统进行变更前后也采用阶段性备份的方式，用于较长时间的保存审

计日志和其他重要信息。

5.4.6 审计收集系统

湖南CA可以审计湖南CA认证体系内任何其认为有必要监控和审计的系统。

5.4.7 对导致事件实体的通告

湖南CA对审查中发现的攻击现象将做详细记录，在法律许可的范围内追溯攻击者或肇事者，并保留采取相应对策措施的权利，如：切断对攻击者或肇事者已经开放的服务、提请司法部门处理等。

湖南CA有权决定是否对导致事件的实体进行通告。

5.4.8 脆弱性评估

湖南CA每年将对系统进行脆弱性评估，以降低系统运行的风险。

5.5 记录归档

5.5.1 归档记录的类型

湖南CA会对CA的数据库定期存档，间隔时间由湖南CA自行决定，存档的内容包括湖南CA发行的证书和CRL、审查数据记录、证书申请审批资料等。（签名私有密钥由证书持有者保存，有关私有密钥的保管责任由证书持有者承担）。

5.5.2 归档记录的保存期限

所有归档记录的保存期一般为证书失效后五年。

5.5.3 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能接近它们。湖南CA保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力等的破坏。

5.5.4 归档文件的备份程序

所有存档文件的数据库除了保存在湖南CA的主要存储库，还将在机房以外的地方保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有授权的工作人员才能在监督的情况下，对档案进行读取操作。湖南CA在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

5.5.5 记录时间戳要求

所有记录都要在存档时加载具体准确的时间标识以表明存档时间。系统产生的记录，用标准时间加盖时间戳。

5.5.6 获得和检验归档信息的程序

湖南CA每年会组织专人检验归档信息的完整性。

5.6 电子认证服务机构密钥更替

5.6.1 密钥转换定义

在这里密钥转换是指当湖南CA根证书到期而需要更换根密钥对时所采取的措施。湖南CA根密钥对由加密机产生。证书到期更换密钥时将签发3张证书。

- 使用旧的私有密钥对新的公钥及信息签名生成证书；
- 使用新的私有密钥对旧的公钥及信息签名生成证书；
- 使用新的私有密钥对新的公钥及信息签名生成证书。

通过以上 3 张证书达到密钥更换的目的，使新旧证书之间互相认证、信任。

5.6.2 根证书有效期

湖南CA根证书有效期为20年。在湖南CA证书到期之前，湖南CA将对根私有密钥进行更换。密钥转换程序在旧密钥对向新密钥对的转换起着过渡的作用。湖南CA密钥转换采用以下方式：

- 湖南 CA 将在证书到期前的 60 天内停止颁发新的证书；
- 旧的湖南 CA 证书到期后，湖南 CA 将用新的 CA 密钥对签发证书。

5.6.3 CRL

湖南CA将继续使用旧的CA根私有密钥签发新的的CRL，直到由旧的CA根私有密钥签发的证书到期为止。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

发生故障时，湖南 CA 将按照灾难恢复计划实施恢复。

5.7.2 计算资源、软件或数据的损坏

湖南 CA 遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难,湖南 CA 将按照灾难恢复计划实施恢复。具体恢复实施细节由湖南 CA 灾难恢复计划规定。

5.7.3 实体私钥损害处理程序

当湖南 CA 根证书被作废时，湖南 CA 通知订户。

湖南 CA 的根私钥出现损毁、遗失、泄露、破解、被篡改，或者有被第三者窃用的嫌疑时，湖南 CA 应该：

1. 立即向电子认证服务管理办公室和其他政府主管部门汇报，并立即吊销所有已经被签发的证书，更新 CRL 信息，供证书订户和依赖方查询。同时湖南 CA 立即生成新的密钥对，并自签发新的根证书。

2. 新的根证书签发以后，按照本 CPS 关于证书签发的规定，重新签发下级证书和湖南 CA 下级操作子 CA 证书。

3. 湖南 CA 新的根证书签发以后，将会立即通过目录服务器、HTTP 等方式进行发布。

湖南 CA 下级操作子 CA 证书的私钥出现遗失、泄露、破解、被篡改，或者有被第三者窃用的嫌疑时，操作 CA 应该：

1. 立即向湖南 CA 进行汇报并生成新的密钥对和证书请求，向湖南 CA 申请签发新的证书。

2. 立即吊销所有已经被签发的证书，更新 CRL 信息，供证书订户和依赖方查询。

3. 新的根证书签发以后，按照本 CPS 关于证书签发的规定，重新签发操作证书。

4. 新的证书签发以后，将会立即通过湖南 CA 目录服务器、HTTP 等方式进行发布。

证书订户的私钥出现遗失、泄露、破解、被篡改，或者有被第三者窃用的嫌疑时，订户应该按照本 CPS 的规定，首先申请证书吊销，并按照规定重新申请新的证书。

5.7.4 灾难后的业务连续性能力

湖南 CA 拥有一套较为完善的系统恢复办法，建设有适当的备用系统以恢复所备份的数据和配置文件，除非物理场地出现了毁灭性的、无法恢复的灾难，湖南 CA 能够在出现灾难后最短的时间内恢复其业务能力。

5.8 电子认证服务机构或注册机构的终止

因各种原因，湖南 CA 需要终止运营时，将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

湖南 CA 在终止服务九十日前，就业务承接及其他有关事项通知各方，包括但不限于湖南 CA 授权的注册机构和证书持有者等。

在终止服务六十日前向中华人民共和国工业和信息化部报告，同时按照相关法律法规的要求办理注销登记手续和业务移交手续。

在 CA 终止期间，采用以下措施终止业务：

- 起草 CA 终止声明
- 通知与 CA 业务停止相关的实体和主管部门；
- 安排业务承接；
- 处理存档文件记录；
- 处理和存储敏感文档；
- 停止认证中心的服务；
- 存档主目录服务器；
- 关闭主目录服务器；
- 关闭从目录服务器；
- 处理并保存加密密钥；
- 处理 CA 主机硬件。

根据湖南 CA 与注册机构签订的协议终止注册机构的业务。

6 认证系统技术安全控制

6.1 密钥对的生成和安装

由于密钥对是安全机制的关键，所以在电子认证业务规则中制定了相

应的规定，确保密钥对的生成、传送、安装等具备保密性、完整性和不可否认性。

6.1.1 密钥对的生成

CA 系统和 RA 系统的密钥对是在国家密码主管部门许可的服务器密码机内部产生。产生 CA 密钥对的时候，必须至少由三位管理员同时在场的情况下由密码机产生，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，其他人员无法获得 IC 卡或相应的密码。

个人和机构订户的签名密钥对由其持有的密码设备（如智能密码钥匙、IC 卡等）产生，加密密钥由密钥管理中心产生。

设备证书订户使用设备程序使用的密码模块提供的密钥对生成功能生成密钥对。

云移动证书签名密钥对，由订户移动终端和云端共同计算产生。服务器端密钥因子在国家密码主管部门许可的服务器密码机中产生，终端密钥因子应包含移动终端设备信息（包含但不限于 MAC 地址、CPUinfo、IMEI 等）、用户因子信息（用户 PIN 码、用户行为特征值等）、随机数等部分计算得到。

6.1.2 私钥传送给订户

订户的签名密钥对在订户的密码设备生成并保管。证书订户的加密私有密钥是在密钥管理中心产生的，通过安全通道传到订户手中的密码设备

中。

云移动证书的签名密钥对，由订户移动终端和云端共同计算产生，通过安全通道协商传输。

6.1.3 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道，经注册机构传递到湖南 CA。订户的加密证书公钥，由 KMC 通过安全通道传递到 CA 中心。

从 RA 到 CA 以及从 KMC 到 CA 的传递过程中，采用国家密码主管部门许可的加密设备、通讯协议及密钥算法建立加密信道传输，保证了信息传输过程中数据的安全性。

6.1.4 电子认证服务机构公钥传送给依赖方

依赖方可以从湖南 CA 的网站(http://www.hunca.com.cn)下载根证书和 CA 证书，从而得到 CA 的公钥。

6.1.5 密钥的长度

湖南 CA 遵从国家法律法规、政府主管机构等对密钥长度的明确规定和要求，目前湖南 CA 电子认证系统支持签发 SM2-256、RSA-2048 密钥的证书，将根据用户的需求为订户提供相应密钥类型的证书。

6.1.6 公钥参数的生成和质量检查

公钥参数由国家密码主管部门许可的加密设备生成，湖南 CA 在采购这

些设备时要求其必须具有国家密码主管部门的相应资质，并遵从国家密码主管部门发布的《证书认证系统密码及相关安全技术规范》以及其他相关规范和标准要求，如对生成的公钥参数的质量检查标准，这些设备内置的协议、算法等均已达到足够的安全等级要求等。

6.1.7 密钥使用目的

订户的签名密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等，加密密钥对可以用于信息加密和解密。

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

在湖南 CA 证书服务体系中的密钥用途和证书类型紧密相关。

- 湖南 CA 的签名密钥用于签发 RA 证书和证书废止列表（CRL）；
- RA 的签名密钥用于确认 RA 所做的审批证书等操作；
- 签名密钥用于提供网络安全服务，如信息在传输过程中不被篡改、接收方能够通过数字证书来确认发送方的身份、发送方对于自己发送的信息不能抵赖等；
- 加密密钥用于对需在网络上传送的信息进行加密，保证信息除发送方和接受方外不被其他人窃取、篡改。

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

湖南 CA 使用国家密码主管部门许可的产品，密码模块的标准符合国家

规定的要求。

湖南 CA 所用的密码设备都是经国家相关部门认可的产品，其安全性达到以下要求：

- 接口安全：不执行规定命令以外的任何命令和操作；
- 协议安全：所有命令的任意组合，不能得到私钥的明文；
- 密钥安全：密钥的生成和使用必须在硬件密码设备中完成；
- 物理安全：密码设备具有物理防护措施，任何情况下的拆卸均立即销毁在设备内保存的密钥。

6.2.2 私钥的多人控制

根 CA 系统的私钥的生成、更新、吊销、备份和恢复等操作采用多人控制机制，即采取五选三方式，将私钥的管理权限分散到三张密码机密钥存储卡和二张管理卡中，只有其中三人以上在场并许可的情况下，才能对私钥进行上述操作。

订户的私钥由订户自己通过终端密码设备控制。云移动证书的签名密钥对由订户终端和云端共同控制。

6.2.3 私钥托管

订户加密证书对应的私钥由密钥管理中心 KMC 托管。订户的签名证书对应的私钥由自己保管，密钥管理中心不负责托管。

KMC 严格保证订户加密密钥对的安全，密钥以密文形式保存，密钥库具有最高安全级别，禁止外界非法访问。

6.2.4 私钥备份

订户的签名私钥湖南 CA 和 KMC 都不备份。加密私钥由 KMC 备份，备份数据以密文形式存在。

订户移动终端和云端各自备份各自的私钥因子。

6.2.5 私钥归档

湖南 CA 的根密钥对到期后，湖南 CA 将对过期密钥进行归档。归档的 CA 密钥对保存在服务器密码机的硬件密码模块中，并且确保归档后的的 CA 密钥不会再用于生产系统中。当归档 CA 密钥对达到归档的保管期限之后，湖南 CA 将按照本 CPS6.2.10 所述的方法进行安全的销毁。湖南 CA 规定过期的密钥对将被归档保存至少 10 年。

订户密钥对的归档是将已过生命周期或决定暂不使用的加密密钥以密文形式保存在数据库中，并通过数据库备份出来进行归档保存，归档后的密钥形成历史信息链，供查询或恢复。

KMC 提供过期的托管加密私有密钥的存档服务。

6.2.6 私钥导入、导出密码模块

在湖南 CA 证书服务体系中，使用湖南 CA 的专用软件可以把私有加密密钥导入密码模块中。

私有密钥无法从硬件或软件密码模块中导出。必须通过密码验证之后，才可能使用存储在密码模块中的私有密钥进行加解密操作。

6.2.7 私钥在密码模块中的存储

湖南 CA 的私有密钥必须保存在硬件密码模块中。

6.2.8 激活私钥的方法

湖南 CA 采用硬件设备（加密机）产生、保存 CA 私钥，其激活数据按照本 CPS6.2.2 要求进行分割。

订户使用硬件密码模块产生、保存私钥，订户使用硬件密码模块口令保护私钥，硬件加密模块被加载，密码模块验证口令完成后，私钥被激活。

6.2.9 解除私钥激活状态的方法

一旦私钥被激活，除非这种状态被解除，私钥总是处于活动状态。

湖南 CA 解除私钥激活状态的方式包括退出、切断电源、移开令牌/钥匙。未经授权的任何人员，绝不可以进行相关操作。

订户解除私钥激活状态的方式由其自行决定，例如退出、切断电源、移开令牌/钥匙等。订户必须自行承担其解除私钥激活状态操作的风险和责任。

6.2.10 销毁私钥的方法

湖南 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吊销后，湖南 CA 依照厂商规定，对加密设备进行清空。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。私钥归档的操作按照本 CPS 的规定处理。

订户的私钥不再被使用，或者与私钥相对应的公钥到期或者被吊销后，由订户决定其销毁方法，订户必须保证有效销毁其私钥，并承担有关的责任。涉及到密钥到期后保存和归档的，订户必须按照本 CPS 的规定执行。

6.2.11 密码模块的评估

湖南 CA 使用国家密码主管部门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，接受其颁布的各类标准、规范、评估结果等各类要求。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

订户证书中的公钥包括签名证书中的公钥和加密证书中的公钥。它们由湖南 CA 和密钥管理中心定期归档。

6.3.2 证书操作期和密钥对使用期限

所有订户证书的有效期和其对应的密钥对的有效期都是一致的。

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，证书存储介质（如：U-KEY）出厂时设置了缺省的 PIN 值。湖南 CA 推荐订户使用强口令来保护私钥的安全性，建议订户不要使用简单重复的数字。

云移动证书使用移动终端设置 PIN 码，输入正确的 PIN 码来启动湖南

CA 手机盾 APP。

6.4.2 激活数据的保护

如果订户证书使用口令或 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

只有在拥有证书介质并知道证书介质的 PIN 值时才能激活证书存储介质，进而使用私钥。

只有拥有移动终端设备并知道 PIN 值才能激活湖南 CA 手机盾 APP，进而调用订户移动终端和云端的私钥。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

湖南 CA 的数字证书签发系统的数据文件和设备由湖南 CA 系统管理员维护，未经授权的其它人员不能操作和控制湖南 CA 系统，以保证系统处于安全可信的运行状态；湖南 CA 系统部署在多级不同厂家的防火墙之内，确保系统网络安全。湖南 CA 系统密码有最小密码长度要求，而且必须符合复杂度要求，湖南 CA 系统管理员定期更改系统密码。

6.5.2 计算机安全评估

湖南 CA 使用的密码设备是通过国家密码管理局批准生产的密码设备，系统建设方案经过国密局的审核，湖南 CA 数字证书认证系统和密钥管理系统通过了国家密码管理局的安全性审查和鉴定，完全符合国家相关安全性规范要求。

6.6 生命周期技术控制

从设计到实施，系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计，使用的算法和密码设备均通过了主管部门鉴定，使用了基于标准的强化安全通信协议确保了通信数据的安全。在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施，整个系统安全可靠。

6.6.1 系统开发控制

系统开发采用先进的安全控制理念，同时应兼顾开发环境的安全、开发人员的安全、产品维护期的配置管理安全。系统设计和开发运用软件工程的方法，做到系统的模块化和层次化，系统的容错设计采用多路并发容错方式，确保系统在出错的时候尽可能不停止服务。

湖南 CA 的软件设计和开发过程遵循以下原则：

- 第三方的验证和审核
- 安全风险和可靠性设计

6.6.2 安全管理控制

湖南 CA 的配置以及任何修改和升级都会记录在案并进行控制，并且湖南 CA 采取一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。

6.6.3 生命期的安全控制

在 CA 策略中对系统运行时的一些参数，包括：订户注册信息的有效期、证书请求的有效期等，当相关事件发生时系统应采取对策进行配置。CA 管理员就可以对这些策略进行设置实现对证书生命期的安全控制。

6.7 网络的安全控制

系统网络安全的主要目标是保障网络基础设施、主机系统、应用系统及数据库运行的安全。湖南 CA 有防火墙、病毒防治、入侵检测以及其他访问控制机制保护，其配置只允许已授权的访问。

6.8 时间戳

数字时间戳（DTS：Digital Time Stamp）是对时间信息的电子签名，主要用于实现确定在某一时间某个文件确实存在和确定多个文件在时间上的逻辑关系功能。湖南 CA 提供的时间源服务采用国家的标准时间源，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

- X.509：V3

7.1.2 证书标准项

- **证书序列号**

唯一标识该证书的一组字符

- **证书有效期**

证书的有效期根据协议规定定义。

- **主题**

为证书订户申请证书时所填写的申请信息，即订户的甄别名。详细请参看§3.1节。

- **发行者**

CN=HUNANCA

C=CN

CN= HUNANCASM2

C=CN

7.1.3 证书扩展项

1、证书扩展项

- 颁发机构密钥标识符（Issuer Unique Identifier）：此域用在当同一个 X.500 名字用于多个认证机构时，用来唯一标识签发者的 X.500 名字。
- 主题密钥标识符（Subject Unique Identifier）：此域用在当同一个 X.500 名字用于多个证书持有者时，用来唯一标识证书持有者的 X.500 名字。
- 密钥使用：指定各种密钥的用法：电子签名，不可抵赖，密钥加密，数据加密，密钥协议，验证证书签名，验证 CRL 签名，只加密，只解密，只签名。
- CRL 发布点：由湖南 CA 定义的 CRL 发布点。

2、自定义扩展项

针对不同的证书应用服务湖南 CA 自定义了一些扩展项

- 工商营业执照：用来记录企业营业执照或统一社会信用代码
- 社保编号：指定企业的社保编号。
- 附加号：证书应用项目的特殊定制
- 企业扩展号：证书应用项目的特殊定制
- 项目编号：证书应用项目的编码

7.1.4 算法对象标识符

符合国家密码主管部门批准的算法对象标识符。

7.1.5 名称形式

采用 X.500 甄别名格式，详看§3.1 节。

湖南 CA 数字证书中的主体 Subject 的 X.500 DN 是 C=CN 命名空间下的 X.500 目录唯一名字，各属性的编码一律使用 UTF8String。

主体 Subject 的 X.500 DN 支持多级 O、OU 和 CN，其格式如下：

- C（Country）应为 CN，表示中国；
- O（Organization）中的内容分为 2 种：
  a) 证书主体或者证书主体所属单位具有明确的上一级单位，则应为其上一级单位的名称全称；
  b) 不存在 a）中所述的上一级单位，则应为证书主体或者证书主体所属单位的所在省、市、直辖市名称全称；
- OU（Organization Unit）应为证书主体或者证书主体所属单位的名称全称；
- CN（Common Name）中的内容分为如下几种：
  a) 个人证书中应为证书主体的标准名称；
  b) 单位机构证书中应为证书主体单位的标准名称；
  c) 设备证书应为证书主体设备的域名名或 IP 地址或者设备编码；
- E 代表电子邮箱地址，Email 仅在邮件证书的 DN 中存在，应为证书

主体的有效电子邮件地址。

- L 代表城市（乡镇）名
- S 代表省市

7.1.6 名称限制

证书名称的使用采用实名制，要求证书名称与证书持有者所提交的各种证件原件、复印件、证明材料、印鉴等必须相符。

7.2 证书吊销列表

湖南 CA 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。

7.2.1 版本号

X.509：V2。

7.2.2 CRL 和 CRL 条目扩展项

CRL 扩展项：颁发机构密钥标识符 Authority Key Identifier。

CRL 条目扩展项：不使用 CRL 条目扩展项

7.3 在线证书状态协议

7.3.1 版本号

Koal OCSP V1.5.2。

7.3.2 OCSP 扩展项

暂无扩展项。

8 认证机构审计和其他评估

8.1 评估的频率或情形

1、根据《中华人民共和国电子签名法》、《电子认证服务管理办法》等相关法律法规的要求，接受上级主管部门定期的评估和检查。

2、湖南 CA 根据国家主管部门的要求、国家相关标准和本 CPS 的规定，按照湖南 CA 的内部评估审计制度，每年至少执行一次内部的评估审计，包括对湖南 CA、湖南 CA 授权的注册机构和其他关联服务机构的评估审计。

湖南 CA 内的关联实体，包括 RA 以及其他湖南 CA 授权的证书服务机构或其他形式的关联体，都必须遵循本 CPS 的相关规定，并接受湖南 CA 对其所有的流程和操作进行审计，检验其是否符合本 CPS 和与之相关的湖南 CA 在授权协议、公示过的认证服务政策等方面的规定。湖南 CA 对关联实体的评估，一般为一年一次，评估人员由湖南 CA 根据需要指派，湖南 CA 在和所有单位的授权协议中，都应对此作出明确规定。评估人员必须熟悉湖南 CA 的规范和认证服务的相关知识，了解运行安全的基本知识，按照湖南 CA 的规范、协议、履行责任业务等情况，独立、公正地对关联实体作出评估。

湖南 CA 授权的证书服务机构可以根据协议，对下属的关联实体进行评估，有权根据上级的评估结果和自己的评估结果，取消对下属单位的授

权或重新授权。

8.2 评估者的资质

1、湖南 CA 无条件接收上级主管部门的评估。对湖南 CA 实施评估的评估者所具有的资质和经验，由主管部门决定。

2、在进行内部评估审计时，湖南 CA 要求评估人员至少具备认证机构、信息安全审计的相关知识，熟悉本 CPS 的规范，以及具备计算机、网络、信息安全等方面的知识和实际工作经验。内部评估审计由湖南 CA 运营安全策略管理委员会负责组织实施。

如果湖南 CA 认为有必要聘请外部的审计者实施内部评估，那么该审计者应该具备以下的资质：

* 必须是经许可的、有营业执照的评估机构，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、标准和规范；

* 具备检查系统运行安全和可靠性的专业技术和工具；

* 熟悉认证机构的管理和运营模式以及相关法律法规。

8.3 评估者与被评估者之间的关系

1、外部评估者(上级主管部门或者其委托的其他机构)和湖南 CA 之间是独立的关系，没有任何的业务、财务往来，或者其它任何利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对湖南 CA 进行评

估。

2、湖南 CA 的内部评估者，与被评估的对象之间，也应是独立的关系，没有任何的利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对被评估的对象进行评估。

湖南 CA 可以根据需要，选择专业、公正、客观的专业审计评估机构，协助进行内部评估。

8.4 评估内容

1、湖南 CA 按照上级主管部门依法提出的评估要求和规范，接受其任何内容的评估。

2、湖南 CA 内部评估审计的内容包括但不限于以下方面：

* 操作的规范性：是否制订和公布 CPS；是否按照 CPS 来制订相关的操作规范和运作协议；是否按照 CPS 及相关操作规范和运作协议开展业务

* 服务的完整性：密钥和证书生命周期的安全管理、证书吊销和挂起的操作、业务系统的安全操作、业务操作标准审查、订户资料的保密和存储管理、售后服务的标准和规程等。

* 安全管理控制：物理环境的安全控制、数据和信息的安全管理、密钥安全管理、人员的安全控制、建筑设施的安全控制、软硬件设备和存储介质的安全控制、系统和网络的安全控制、系统开发和维护的安全控制、灾难恢复和备份系统的管理、审计和归档的安全管理等。

8.5 对问题与不足采取的措施

1、上级主管部门评估完成后，湖南 CA 必须根据评估的结果检查缺失和不足，根据其提出的整改要求，提交修改和预防措施以及整改计划书，并接受评估部门对整改计划的审查，以及对整改情况的再次评估。

2、湖南 CA 完成内部评估后，评估人员需要列出所有问题项目的详细清单，由评估人员和被评估部门或对象共同讨论有关问题，并将结果书面通知湖南 CA 运营安全策略管理委员会和被评估对象。被评估对象必须根据评估的结果检查缺失和不足，提交修改和预防措施以及整改计划书，并接受湖南 CA 运营安全策略管理委员对整改计划的审查，以及对整改情况的再次评估。

8.6 评估结果的传达与发布

1、信息产业主管机构在完成评估后，按照法律法规的要求对评估结果进行处理。

2、湖南 CA 的内部评估结果在与被评估对象的相关人员进行讨论确定后，将其视为机密资料进行保存，只有被评估对象和湖南 CA 安全管理委员会可以查阅。非经湖南 CA 运营安全策略管理委员批准，任何人不得将评估内容和结果泄露给其他无关的第三方，否则当事人将承担由此引起的一切后果和责任。

在必要的情况下，对湖南 CA 关联实体评估的结果，其通知方法将在湖南 CA 和被评估实体的独立协议中确定。

任何第三方向被评估实体通知评估结果或者类似的信息，都必须事先明确的向湖南 CA 表明通知的目的和方式，并征得湖南 CA 运营安全策略管理委员的同意，法律另有规定的除外；湖南 CA 保留在此方面所享有的权力。

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

湖南 CA 对数字证书的收费标准参照市场和湖南省物价主管部门批准的收费标准执行。根据证书实际应用需要，湖南 CA 在不高于收费标准的前提下可以对证书价格进行适当调整。

9.1.2 证书查询费用

在证书有效期内，对该证书信息进行查询，湖南 CA 不收取查询费用。

9.1.3 证书吊销或状态信息的查询费用

查询证书是否吊销，湖南 CA 不收取信息访问费。

对于 OCSP 服务和其他定制的证书状态查询服务，湖南 CA 根据与客户的服务协议要求进行收费。

9.1.4 其他服务的费用

湖南 CA 保留收取其他服务费的权利。

9.1.5 退款策略

在实施证书操作和签发证书的过程中，湖南 CA 遵守并保持严格的操作程序和退款策略。一旦订户接受数字证书，湖南 CA 将不办理退证退款手续。

如果订户在证书服务期内退出数字证书服务体系，湖南 CA 将不退还剩余时间的服务费用。

9.2 财务责任

湖南 CA 保证具有维持、运作和履行其责任的财务能力。湖南 CA 有能力承担对订户、依赖方等造成的责任风险，并依据本电子认证业务规则规定的方式进行赔偿。

9.3 业务信息保密

9.3.1 保密信息范围

保密的业务信息包括但不限于以下方面：

a) 在双方披露时标明为保密(或有类似标记)的；

b) 在保密情况下由双方披露的或知悉的；

c) 双方根据合理的商业判断应理解为保密数据和信息的；

d) 以其他书面或有形形式确认为保密信息的；

e) 从上述信息中衍生出的信息。

对于湖南 CA 来说，保密信息包括但不限于以下方面：

a) 最终订户的私人签名密钥；

b）保存在审计记录中的信息；

c）年度审计结果；

除非法律有要求，由湖南 CA 掌握的，除作为证书、CRL、认证规则等被明确发布之外的所有个人和公司的信息均需要保密。

湖南 CA 不保存任何证书应用系统的业务信息或交易信息。除非法律明文规定，湖南 CA 没有义务公布或透露订户数字证书以外的信息。

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、证书使用操作指南等资料中公布的信息是可以公开的。而且湖南 CA 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。

湖南 CA 在目录服务器中公布的证书信息及其状态信息，不属于保密信息。

当湖南 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，湖南 CA 可以按照法律、法规或规章条款以及法院的判定要求，向执法部门提供相关的保密信息。这种信息披露不视为违反了保密的要求和义务。

9.3.3 保护保密信息的责任

湖南CA 与湖南CA 授权的注册机构之间、湖南CA 与证书持有者之间、湖南CA 授权的注册机构与证书持有者之间的协议、往来函和商务协定等，除非法律明确规定，一般不能在未经另一方许可的前提下擅自公开。

对湖南CA 或湖南CA 对注册机构的审计报告、审计结果等相关信息是保密信息，除了湖南CA 授权和信任的员工，不能泄露给其他任何人。这些信息除了用于审查目的或法律规定的目的外，不能用于其他用途。

有关湖南CA 电子认证服务机构运作的信息只能在严格指定的情况下，才能传授给湖南CA 授权的员工。

控制发证机构软硬件操作的安全措施和管理证书服务及注册服务的安全措施。

除非法律明文规定，湖南CA 没有义务公布或透露证书持有者证书以外的信息。

湖南CA的每个员工都要接受信息保密方面的培训。

9.4 个人隐私保密

9.4.1 隐私保密方案

除非证书申请人主动提供，湖南CA保证不会截取任何证书申请人的资料。

湖南CA应保护证书申请人所提供的，证明其身份的资料。湖南CA应采取必要的安全措施防止证书申请人所提供的资料被遗失、盗用与篡改。

9.4.2 作为隐私处理的信息

证书申请人提供的不构成数字证书内容的资料被视为隐私信息。

9.4.3 不被视为隐私的信息

与证书持有者证书相关的信息均为公开信息，可以通过湖南CA目录服务等方式向外公布。

9.4.4 保护隐私的责任

接收到隐私信息的参与者有责任保护隐私信息不被泄漏、使用或发布给第三方。在法律法规和公共权力部门通过合法程序要求下，湖南CA可以向特定的对象公布隐私信息，湖南CA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

使用隐私信息，须告知并获得隐私所有人或机构的同意。

9.4.6 依法律或行政程序的信息披露

当湖南CA在任何法律、法规或规章的要求下，或在法院的要求下必须提供证书申请人的特定资料或隐私信息时，湖南CA按照法律、法规或规章的要求或法院的要求，向执法部门公布相关信息，湖南CA无须承担任何责任。这种提供不能被视为违反了隐私保护的责任和义务。

9.4.7 其他信息披露情形

其他信息的披露遵循国家的相关规定处理。

9.5 知识产权

湖南CA 享有并保留对证书以及湖南CA 提供的全部软件、资料、数据等的著作权、专利申请权等全部知识产权。因此，湖南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通。

按本CPS 的规定，所有与湖南CA 发行的证书和湖南CA 提供的软件相关的一切版权、商标和其他知识产权均属于湖南CA 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湖南CA 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。

在没有湖南 CA 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 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。

9.6 陈述与担保

除非湖南 CA 做出特别约定，若本电子认证业务规则的规定与湖南 CA 制定的其他相关规定、指导方针相互抵触，以本电子认证业务规则为准。在湖南 CA 与包括订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。

9.6.1 电子认证服务机构的陈述与担保

湖南 CA 在提供电子认证服务活动过程中的承诺如下：

a) 湖南 CA 遵守《中华人民共和国电子签名法》及相关法律法规的规定，接受国家工业和信息化部的业务监督和指导，对所签发的数字证书承担相应的法律责任。

b) 湖南 CA 保证使用的系统及密码符合国家政策与标准，保证其 CA 本身的签名私钥在内部得到安全的存放和保护,建立和执行的安全机制符合国家政策的规定。

c) 除非已通过湖南CA证书库发出了湖南CA的私钥被破坏或被盗的通知，湖南 CA 保证其私钥是安全的。

d) 湖南 CA 签发给订户的证书符合湖南 CA CPS 规定的所有实质性要求。

e) 湖南 CA 将向证书订户通报任何已知的、将在本质上影响证书的有效性和可靠性事件。

f) 湖南 CA 将及时吊销证书，并发布到 CRL 上供订户查询。

g) 证书公开发布后，湖南 CA 向证书依赖方证明，除未经验证的订户信息外，证书中的其他订户信息都是准确的。

9.6.2 注册机构的陈述与担保

湖南 CA 的注册机构在参与电子认证服务过程中的承诺如下：

a) 提供给证书订户的注册过程完全符合湖南 CA CPS 的所有实质性要

求。

b) 在湖南 CA 生成证书时，不会因为注册机构的失误而导致证书中的信息与证书申请人的信息不一致。

c) 注册机构将按本 CPS 的规定，及时向湖南 CA 提交证书申请、吊销、更新等服务请求。

9.6.3 订户的陈述与担保

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

a) 订户已阅读并知悉本《电子认证业务规则》的所有条款以及与其证书相关的证书使用政策,并同意承担证书持有人有关证书的相关责任和义务。

b) 订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，并可供湖南 CA 或注册机构检查和核实。

c) 订户应当妥善保管私钥，采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件的发生。

d) 订户对使用私钥的行为负责。

e) 一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄密以及其他情况，订户应立刻通知湖南 CA 和注册机构，及时申请采取证书吊销等处理。

f) 订户已知其证书被冒用、破解或被他人非法使用时，应及时通知湖南 CA 吊销其证书。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉本《电子认证业务规则》的条款以及和订户数字证书相关的证书政策，并确保本身的证书只用于申请时预定的目的。

依赖方在信赖其他订户的数字证书前，必须采取合理步骤，查证订户数字证书及数字签名的有效性。

证书依赖方对证书的信赖行为就表明他们已阅读并知悉本《电子认证业务规则》的所有条款，并同意承担证书依赖方有关证书使用的相关责任和义务。

9.6.5 其他参与者的陈述与担保

其他参与者的陈述与担保同§9.6.4。

9.7 担保免责

下列情况之一的，应当免除湖南 CA 之责任。

a) 如果证书申请人故意或无意地提供了不准确或不真实或不完整的信息，又根据正常的流程提供了必须的审核文件，得到了湖南 CA 签发的数字证书，由此引起的法律和经济纠纷应由证书申请人全部承担。湖南 CA 不承担由此引起的法律和经济责任，但可以根据受害者的请求提供协查帮助。

b) 湖南 CA 不承担任何未经授权的人或组织以湖南 CA 名义编撰、发表或散布的不准确、不实或不可信赖的信息所引起的法律责任。

c) 在法律许可的范围内，根据司法程序要求如实提供网上业务中“不

可抵赖”的数字签名证据，湖南 CA 不承担由此引起的任何法律责任。

d) 湖南 CA 不对任何一方信赖证书或使用证书在业务操作过程中引起的直接或间接的损失承担责任。

e) 湖南 CA 和注册机构不是证书持有人或依赖方的代理人、受托人、管理人或其他代表。湖南 CA 和证书持有人间的关系以及湖南 CA 和依赖方间的关系并不是代理人或委托者的关系。证书持有人和依赖方都没有权利以合同形式或其他方式让湖南 CA 承担信托责任。

f) 由于不可抗力因素导致湖南 CA 暂停、终止部分或全部数字证书服务，湖南 CA 不承担赔偿或补偿责任。关于不可抗力的描述参见§ 9.16.5。

g) 由于非湖南 CA 原因造成的设备故障、网络中断导致证书报错、交易中断或其他事故造成的损失，湖南 CA 不向任何方承担赔偿或补偿责任。

h) 湖南 CA 已谨慎的遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的，湖南 CA 不承担相关责任。

i) 订户因证书丢失、私钥泄漏等原因需办理挂失、注销手续。在订户办理证书挂失或注销手续前及自订户申请办理挂失或注销起到生效时 24 小时内造成的损失，湖南 CA 不承担相关责任。

j) 湖南 CA 对各类证书的适用范围作了规定，若证书被超出范围使用或被用于其他未被湖南 CA 允许的用途，湖南 CA 不承担任何法律责任。

9.8 有限责任

如果湖南 CA 根据本 CPS 或任何法律规定，以及司法判定须承担赔偿或补偿责任的，湖南 CA 将按照相关法律法规的规定、仲裁机构的裁定或法院的判决承担相应的赔偿责任。

9.9 赔偿

湖南 CA 按照本《电子认证业务规则》§9.7 和§9.8 条款具有担保免责和承担有限赔偿责任。湖南 CA 在与订户和依赖方签定的协议中，对于因订户或依赖方的原因造成的损害不具有赔偿义务。

湖南 CA 对于湖南 CA 的数字证书订户有限赔偿责任的赔偿金额上限暂定为该订户实缴该数字证书年服务费的十倍。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的责任均有封顶而不考虑数字签名和交易处理等有关的其他索赔的数量。当超过责任封顶时，可用的责任封顶将首先分配给最早得到索赔解决的一方。湖南 CA 没有责任为每个证书支付高出责任封顶的赔偿，而不管责任封顶的总量在索赔提出者之间如何分配的。

证书订户和依赖方在使用或信赖证书时，若有任何行为或疏漏而导致湖南 CA 和注册机构名誉或经济损失，订户和依赖方应承担赔偿湖南 CA 和有关各方名誉或经济损失的责任。

订户接受证书就表示同意在以下情况下承担相应赔偿责任。

a) 未向湖南 CA 提供真实、完整和准确的信息，而导致湖南 CA 或有关

各方损失。

b) 未能保护订户的私钥,或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用并造成损失。

c) 在知悉证书密钥已经失密或者可能失密时，未及时告知湖南 CA，并终止使用该证书，而导致湖南 CA 或有关各方损失。

d) 订户如果向依赖方传递信息时表述有误,而依赖方用证书验证了一个或多个数字签名后理所当然地相信这些表述,订户必须对这种行为的后果负责。

e) 证书的非法使用，即违反湖南 CA 对证书使用的规定，造成了湖南 CA 或有关各方的利益受到损失。

9.10 有效期与终止

9.10.1 有效期限

湖南 CA 的电子认证业务规则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，最新版本请访问湖南 CA 网站，对具体订户不做另行通知。

9.10.2 终止

当新版本的《湖南 CA 电子认证业务规则》正式发布生效时，旧版本将自动终止。

9.10.3 效力的终止与保留

《湖南 CA 电子认证业务规则》的某些条款在终止后继续有效，如知识产权承认和保密条款。另外，终止后各参与方应返还保密信息给其拥有者。

9.11 对参与者的个别通告与沟通

湖南CA 及其注册机构在必要的情况下，如在主动吊销订户证书、发现订户将证书用于规定外用途及订户协议的行为时，会通过适当方式，如电话、电邮、信函、传真等，个别通知订户、依赖方。

9.12 修订

湖南 CA 有权在合适的时间修订、修改或改变本认证业务规则声明中的任何术语、条件和条款，而且无需通知任何相关方。

湖南 CA 有权在湖南 CA 的自主数据库中设置和公布修改结果，或以其他方式（如修改 CPS 版本的形式在网站上）公布。

所有的修订、修改和改变在公布后立刻生效。证书持有者如不在修改结果公布后的 30 日内申请废止证书，就视为同意这种修正、修改和变化。

所有以书面形式提供给证书持有者的资料，按以下规则发送：

- 接受者是公司或其它单位组织则向其登记的联系地址或办公室发送信息；
- 接受者是个人则向其申请书上填报的地址发送；
- 这些通知可能用快递或挂号信的方式发送。湖南 CA 有权选择通过电子邮件或其他方式向证书持有者发送通知，邮件地址在证书持有

者申请证书时已注明。

订户发送给湖南 CA 的通知应以书面形式传递。所有这些通知应采用快递或挂号信的方式发送。若通过电子邮件方式发送通知给湖南 CA，则这种通知只有在湖南 CA 收到订户的电子邮件通知后 24 小时内，收到相应的书面确认材料，方为有效。

9.12.1 修订程序

1、湖南 CA 发现 CPS 中所列条款不能适应运营的实际需求，或与现行法律相抵触；

2、将现存问题反馈给 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策略管理委员会讨论；

5、运营安全策略管理委员会审查修改意见，如果不通过则提出意见反馈给 CPS 编写小组；

6、CPS 编写小组根据反馈意见进一步完善。修改意见经运营安全策略管理委员会审查通过后，发布更新。

7、更新后的CPS自公布之日起30日内向工业和信息化部备案。

9.12.2 通告机制和期限

本电子认证业务规则在湖南 CA 的网站上发布。版本更新时，最新版本的《湖南 CA 电子认证业务规则》会在湖南 CA 的网站及时公布，对具体个人和单位订户不做另行通知。

9.12.3 必须修改业务规则的情形

当管辖法律、法规、适用标准及操作规范等有重大改变时，必须修改本电子认证业务规则。

9.13 争议处理

湖南 CA、订户、依赖方等实体在电子认证活动中产生争端可按照以下步骤解决：

1、当事人首先通知湖南 CA,根据本 CPS 中的规定，明确责任方；

2、由湖南 CA 相关部门负责与当事人协调；

3、若协调失败，可以通过仲裁或司法途径解决；

4、任何因与湖南 CA 或授权的注册机构就本 CPS 所产生的任何争议而提起诉讼的，受湖南省数字认证服务中心有限公司所在地的人民法院管辖。

9.14 管辖法律

本电子认证业务规则在各方面服从中国法律和法规的管辖和解释，包括《中华人民共和国电子签名法》及《电子认证服务管理办法》等。

9.15 与适用法律的符合性

无论在任何情况下，本电子认证业务规则的执行、解释、翻译和有效性均应遵守和适应中华人民共和国的相关法律和法规。如有不符之处，应以中华人民共和国的相关法律和法规为准。

9.16 一般条款

9.16.1 完整协议

CPS、订户协议及依赖方协议及其补充协议将构成湖南CA 信任域参与者之间的完整协议。

9.16.2 转让

湖南CA、注册机构、订户及依赖方之间的责任、义务不能通过任何形式转让给其他方。

9.16.3 分割性

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

9.16.4 强制执行

免除一方对合同某一项的违反应该承担的责任，不意味着继续免除或未来免除这一方对合同其他项的违反应该承担的责任。

9.16.5 不可抗力

不可抗力是指不能预见、不能避免并不能克服的客观情况。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风、火灾等自然现象；也可以是社会现象、社会异常

事件或者政府行为，如合同订立后政府颁发新的政策、法律和行政法规，致使合同无法履行，再如战争、罢工、骚乱等社会异常事件。

在数字证书认证活动中，湖南 CA 由于不可抗力因素而暂停或终止全部或部分证书服务的，可根据不可抗力的影响而部分或全部免除违约责任。其他证书和认证相关各方不得提出异议或申请任何补偿。

9.16.6 其他条款

湖南 CA 对本《电子认证业务规则》拥有最终解释权。