湖北CA电子政务

电子认证服务业务规则

版本 1.1

日期：2012年10月

目　　录

版权声明

对任何复制及传播本文件的请求，请寄往：湖北省数字证书认证管理中心有限公司

地址：湖北省武汉市武昌区水果湖东一路 19 号 邮编：430071 电话：027-87823765(810)

传真：027-87822397 电子邮件：lidan_liu@HBCA.org.cn

本 CPS 的最新版本请参见本公司网站(www.hbca.org.cn),对具体的自然人、政府组织机构不在另行通知。

湖北 CA 运营安全策略委员会负责解释本 CPS.

修订历史

版本	日期	备注	修订人
1．0	2010 年 12 月	根据《电子认证服务管理办法》、《电子政务电子认证服务管理办法》、《电子政务电子认证服务业务规则规范》的各项要求进行制定。	刘力丹
1.1	2012 年 10 月	根据《电子政务电子认证服务管理办法》、《电子政务电子认证服务业务规则规范》等进行制定。	刘力丹

对任何已经或即将涉嫌犯罪而影响湖北 CA 电子政务电子认证服务的组织、单位和个人，湖北 CA 将保留依法追诉的权利。

第一章 概括性描述

1.1 概述

《湖北CA电子政务电子认证服务业务规则》(简称本CPS)接受《电子政务电子认证服务业务规则规范》（国家密码局2010年8月）的约束,全面地规定了湖北CA为各终端实体提供电子政务电子认证服务过程中应遵守的规则和相关法律责任,主要内容有数字证书服务、应用集成支持服务、信息服务、使用支持服务操作规则和安全保障规则、电子政务电子认证服务的法律责任等方面，同时,湖北CA通过本CPS向社会公布我们提供电子政务电子认证服务的基本立场和观点,湖北CA、湖北CA授权机构、湖北CA签约实体、湖北CA员工、证书持有者等认证体系内的所有实体，有责任和义务完整地理解和执行本CPS所规定的相关条款，承担相应的责任和义务。

1.2 遵从规范

本CPS的制定遵从：

《中华人民共和国电子签名法》

《电子认证服务管理办法》

《电子认证服务密码管理办法》

《电子政务电子认证服务管理办法》

《电子政务电子认证服务业务规则规范》

《证书认证系统密码及其相关安全技术规范》

《电子政务数字证书格式规范》

《电子政务数字证书应用接口规范》

湖北CA承诺，根据上述法规制定的本CPS，没有出现与上述法规冲突的条款，没有出现无法执行上述法规要求的条款。

1.3 适用对象

本 CPS 适用对象包括：

- 湖北CA的所有注册机构及下级受理点
- 由湖北CA委托的第三方机构
- 湖北CA的电子政务订户
- 湖北CA的电子政务依赖方

1.4 文档名称与标识

本文档名称全称为《湖北 CA 电子政务电子认证服务业务规则》,本文档内以及湖北 CA 业务范畴所使用的电子政务 CPS 均指本 CPS。

1.5 电子认证活动参与者

1.5.1 湖北 CA

湖北省数字证书认证管理中心有限公司（简称湖北CA）是经湖北省政府批准成立的一家专门从事电子认证服务的认证服务机构，是获得国家信息产业部颁发的《电子认证服务许可证》和国家密码管理局颁发的《电子政务电子认证服务机构许可证》的第三方机构。

湖北 CA 是湖北网络信任体系建设与运营的主体，主要

从事电子政务、电子商务有关的电子认证服务业务，可提供方案设计、技术支撑及咨询培训等信息安全服务，保障电子签名人及电子签名依赖方的身份认证、授权管理及责任认定，保证电子政务及电子商务活动双方身份的真实性、通信信息的保密性、交换数据的完整性、交易行为的不可否认性以及访问权限的可控性。

湖北 CA 采用国家认可的数字证书认证系统，建有高度安全的 CA 中心、密钥管理中心以及先进、可扩展的安全基础设施。公司建立了完善的市场拓展、技术研发、系统运行、客户服务及运营安全保障体系和稳妥的发展机制，业务已经覆盖了国内多个行业，建立了数十个业务受理点。

湖北 CA 将依托服务优势，不断提升电子认证服务的质量，积极拓展新的市场，探索更加优质的服务模式，为电子认证服务业的发展奠定坚实的基础。

1.5.2 注册机构

注册机构是为订户建立注册过程的机构，它的主要职能包含但不限于：

- 对订户进行身份标识和鉴别
- 发起或传递证书注销请求
- 代表湖北 CA 批准更新证书或更新密钥的申请
- 负责证书用户信息的审核、整理汇总、统计分析
- 与上级 CA 进行数据交换，管理和服务下层注册分支机构和下层受理点
- 为订户提供技术支持等有关服务
- 注册机构必须遵守本CPS

1.5.3 受理点

- 受理点是负责审核订户信息、为订户提供技术支持等有关服务的机构。
- 受理点必须遵守本CPS

1.5.4 订户与证书持有者

订户是指申请数字证书并递交了申请材料，证书持有者已经接受了湖北CA签发的数字证书的终端实体，包括有机构、个人、服务器等。机构、个人、服务器必须遵守本CPS

1.5.5 依赖方

依赖方是指需要验证证书和签名的实体。依赖方可验证接收到的经过数字签名的数据电文的完整性和真实性。

1.5.6 其他参与者

其他参与者可能包括一些权威机构，例如：湖北CA在对订户进行身份鉴别的时候，可能需要第三方的权威机构出具身份证明材料。

1.6 证书的用途

1.6.1 支持的证书应用

湖北CA的证书可以用于网络身份认证、网络安全登录、信息保护和通信密钥协商等。还可以用于其他用途，条件是：依赖方根据自己的评估，有充分的理由信任该证书，并确保该证书的使用不违反相关法律、本CPS以及订户协议。

1.6.2 不支持的证书应用

湖北CA的证书只能在不违背相关适用法律的范围内使用，并且不能用于直接导致人员伤亡或者严重破坏环境的应用，例如：核设备的操作、航天器的导航或通信系统、航空管制系统或者武器控制系统等。

1.6.3 证书的类型

湖北 CA 提供如下四种数字证书:

证书类型	通用名	主要用途
个人证书	个人姓名（与身份证上标明的一致）	用于签名和加密、证明身份唯一等
机构证书	机构名称（与合法有效证件上标明的一致）	用于签名和加密、证明身份唯一等
服务器证书	服务器主机名或 IP 地址	保证客户与服务器交互信息安全
代码签名证书	个人姓名（与身份证上标明的一致） 单位名称（与合法有效证件上标明的一致）	使用该证书对软件代码数字签名，用于表示软件代码的开发者身份。

1.7 策略管理

1.7.1 策略管理机构

本 CPS 的管理机构是湖北 CA 运营安全策略委员会，由湖北 CA 运营安全策略委员会负责本 CPS 的制定、发布、更新等事宜。

1.7.2 联系人

湖北CA指定 刘力丹 作为本CPS的联系人，负责处理有关本电子政务电子认证服务业务规则的建议和疑问。

湖北 CA 将对认证业务规则进行严格的版本控制，并由湖北 CA 指定专人负

责。

联 系 人：刘力丹

电　　话：027－87823765(810)

传　　真：027－87822397

地　　址：湖北省武汉市武昌区水果湖东一路十九号

邮箱地址：lidan_liu@HBCA.ORG.CN

邮政编码：430071

1.7.3 电子政务电子认证服务业务规则的审批机关

湖北CA运营安全策略委员会为本CPS的审批管理机构。

1.7.4 电子政务电子认证服务业务规则的审批流程

制定和修改本CPS需要经过以下工作流程:

- 由湖北CA运营安全策略委员会指定人员提名组成制定或修改CPS相应的起草小组人员名单
- 报湖北CA运营安全策略委员会审核批准
- 起草小组开始工作
- 本次制定或修改工作完成后该小组自行解散

发布流程:

- 本CPS文稿提交湖北CA运营安全策略委员会
- 湖北CA运营安全策略委员会全体人员审核
- 提交国家管理部门备案
- 正式发布

本CPS已经在电子政务电子认证服务管理部门备案。

1.8 定义和缩写

下列定义适用于本 CPS:

- 数字证书：Digital Certificate，是经权威的、可信赖的、公正的第

三方湖北 CA 签发的包含拥有公开密钥者信息以及公开密钥的电子文档。

- 湖北 CA（CA）：即 Certificate Authority，或 Certifying Authority，是指颁发用以创建数字签名和公/私密钥对的电子签名认证证书的可信第三方权威机构。
- 注册机构（RA）：Registration Authority，证书的注册机构，是指帮助订户申请证书，批准或拒绝证书申请，注销证书或更新证书。
- 电子政务电子认证服务业务规则（CPS）：Certification Practice Statement，湖北 CA 为电子政务提供数字证书服务操作规范、应用集成支持服务操作规范、信息服务操作规范、使用支持服务操作规范、安全保障规范和电子认证服务的法律责任等方面需要遵循的操作规则描述和说明。
- 证书注销列表（CRL）：Certificate revocation list，一个定期(或根据要求)发行的、并由湖北 CA 经过数字签名的信息列表，用来识别在有效期内提前被注销的证书。
- 私钥：是非对称算法产生的两个密钥中的一个，由最终订户唯一持有，用于制作电子签名。
- 公钥：是非对称算法产生的两个密钥中的一个，绑定在电子签名认证证书中，通过湖北 CA 在公网上发布，用于验证电子签名信息的有效性。
- USB KEY:采用 USB 接口的证书存储介质。

第二章 信息发布和资料库职责

2.1 资料库

湖北CA已经建立了一个允许公众访问的在线资料库，并将其签发的证书以

及证书状态信息（如：撤销信息）发布到该资料库上。

2.2 信息发布

湖北CA已经将下列信息发布到资料库上，允许订户或依赖方进行在线查询：

- 所签发的证书及其状态信息

湖北CA已经将下列信息发布到公司网站上，允许订户或依赖方查询，但不可修改：

- 最新版本的《湖北CA电子政务电子认证服务业务规则》

2.3 发布信息的时间或频率

湖北CA本CPS在改版后即更新发布，一经发布即时生效。对湖北CA 数字证书订户及申请人均具备约束力，对具体个人等终端实体不另行通知。

对于终端订户的证书撤销列表（简称“CRL”），至少每24小时签发一次；湖北CA根证书的证书撤销列表至少每年签发一次，或者当湖北CA的根证书需要撤销时签发证书撤销列表。

在证书签发时，湖北CA 通过目录服务器（Ldap ）自动将该证书公布。

2.4 资料库的访问控制

湖北CA承若，没有故意使用技术手段来限制对以下信息的访问：

湖北CA电子政务电子认证服务业务规则、证书和证书状态信息。

湖北CA已经通过管理制度和授权等技术措施来阻止对资料库的信息进行非授权的添加、删除或修改。

第三章 数字证书服务操作规范

3.1 命名

数字证书注册信息中所有的命名遵循《电子政务数字证书格式规范》的要求。

3.1.1 名字类型

湖北CA签发的证书已经包含湖北CA的名称和订户的名称。出现在主体域的主体名称使用 X.501 可辨识名（Distinguished Name，DN）。

3.1.2 名称意义化的要求

订户在证书中的名称要有一定的实际意义（假名证书除外），例如：机构名称、姓名、电子邮件地址和电话号码等。

3.1.3 订户的匿名或假名

订户在证书中的名称可以是假名但不允许匿名。

3.1.4 不同名字格式的解释规则

不作规定。

3.1.5 名称的唯一性

湖北CA不能将相同主体名称的证书签发给不同的实体。同一个订户可以拥有多个相同主体名称的证书。当出现相同的名称时，以先申请者优先使用，后申请者在唯一标识名称后面加识别码予以区别。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

湖北CA基于满足下面两个条件来证明证书持有者对私钥的持有：

（1）通过证书请求中所包含的数字签名来证明证书持有者与注册公钥对应的私钥，流程如下：

- 证书持有者在客户端生成公私钥对
- 证书持有者应使用其私钥对证书请求信息进行数字签名，并连同公钥一起提交给CA系统
- CA应使用证书持有者公钥验证该签名

（2）证书持有者拥有私钥保护口令，即用户能够使用数字证书进行签名，证明其是拥有私钥。

3.2.2 机构身份的鉴别

当订户是机构的时候，至少需要进行如下鉴别：

- 利用权威第三方提供的身份证明（如经办人的有效身份证件、加盖公章的授权申请文件）或数据库服务，也可以是政府机构发放的合法性文件（如：组织机构代码证等）证明该机构确实存在；同时，订户应提交符合填写规范的《机构证书申请表》。
- 通过电话、邮政信函或与此类似的其他方式确认该机构资料信息的真实性，以及代表机构进行证书申请的个人是否得到足够的授权。

湖北CA对上述材料进行审核和鉴别，作出批准申请或拒绝申请的操作。如批准，将保留相关证明材料的复印件，与申请表一起存档保存。

3.2.3 自然人身份的鉴别

当订户是自然人的时候，至少需要进行如下鉴别：

- 利用权威第三方提供的身份证明（如有效身份证件复印件）或数据库服务，来证明订户的身份；订户应提交符合填写规范的《个

人证书申请表》。

- 通过电话、邮政信函或与此类似的其他方式确认个人信息的真实性，以及代表进行证书申请的个人是否得到足够的授权。

在把证书签发给政府部门中的个人时，湖北CA的注册机构必须确认以下内容：

- 需要通过可靠的方式确保证书持有者所在的组织、部门与证书中所列的组织、部门一致，证书中通用名就是证书持有者的真实姓名。
- 需确认证书持有者属于该组织机构，证书持有者确实被雇佣。

湖北CA对上述材料进行审核和鉴别，作出批准申请或拒绝申请的操作。如批准，将保留相关证明材料的复印件，与申请表一起存档保存。

3.3 密钥更新请求的身份标识与鉴别

3.3.1 常规密钥更新请求的身份标识与鉴别

密钥更新申请者身份标识与鉴别方式如下：

- 申请时，对应的原证书存在并且是由湖北CA注册机构签发
- 用原证书上的证书持有者公钥对申请的签名进行验证
- 基于原注册信息进行身份鉴别

订户也可以选择一般的新证书申请流程进行常规密钥更新，按照要求提交证书申请所需的材料。

3.3.2 撤销后密钥更新请求的身份标识与鉴别

证书撤销后，不能进行密钥更新，此时若订户申请密钥更新，需要重新按新证书申请流程进行身份标识与鉴别。

3.4 证书撤销请求的标识与鉴别

证书撤销申请者必须满足下列条件之一：

- 提供初始身份验证时的申请材料
- 证明拥有需要撤销证书的私钥

湖北CA可以通过电话、传真、邮政信函或其他证明方式等对订户的撤销请求的身份进行鉴别。

申请撤消证书应包括以下流程：

- 证书持有者通过一定的方式向注册机构提交撤消请求
- 注册机构按照《湖北CA电子政务电子认证服务业务规则》规定的方式与证书持有者联系，并对申请人进行身份鉴证，确认要撤消证书的人或组织确实是证书持有者本人或被授权人

如果是因为证书持有者没有履行本CPS所规定的义务，湖北CA撤消证书时，不需要对证书持有者进行身份标识和鉴别。

如果司法机关依法提出证书撤销请求，湖北CA将唯一地以司法机关提供的书面撤销请求文件作为鉴别依据。

3.5 证书生命周期操作要求

3.5.1 证书申请

3.5.1.1 提交证书申请的人

下列人员可以提交证书申请：

- 能够独立承担民事责任的自然人或其授权代表
- 具有独立法人资格机构的授权代表

3.5.1.2 登记过程和责任

湖北CA将对材料进行验证是否真实、充分。

湖北CA保证订户和持有者信息不被篡改、私密信息不被泄露。

所有订户和证书持有者必须明确表示同意订户协议中的内容。

所有订户在申请时，必须提供真实的身份信息。

湖北CA保留对最终实体身份的证明和确认信息。

3.5.2 证书申请处理

湖北CA接到证书申请后：

- 湖北CA按照初始身份鉴别的要求，对订户进行识别和鉴证
- 对订户行为的合法性进行鉴证，确认其申请行为合法授权
- 依据鉴证结果，作出批准或拒绝申请的决定，在24小时内通知订户结果及其相应的原因
- 接受证书申请，将妥善保管订户申请时提交的所有材料

如果同时满足下列三个条件，湖北CA将接受订户的证书申请：

- 成功标识和鉴别了订户的信息
- 确认了行为的合法授权
- 收到了相应的费用

如果发生下列情形之一，湖北CA将拒绝订户的证书申请：

- 不能完成标识和鉴别过程
- 订户不能提供湖北CA需要的补充文件或没有在指定的时间内响应湖北CA的通知
- 未收到相应的费用
- 湖北CA认为批准该申请将会导致湖北CA陷入法律纠纷

3.5.3 证书签发

3.5.3.1 证书签发期间湖北 CA 的行为

- 湖北CA接受订户的证书申请后，基于审核通过的信息进行证书签发
- 证书签发中RA与湖北CA互相进行身份认证并确保申请信息传输的机密性
- 湖北CA验证RA的签发请求，确保是无误后签发证书

3.5.3.2 订户证书签发的通知

湖北CA签发新证书后，及时通知订户其证书已被签发，常用的方式有：

- 面对面的方式
- 呼叫中心、传真、电子邮件方式
- 其他湖北CA 认为安全可行的方式

3.5.4 证书接受

3.5.4.1 证书接受的行为

订户接受证书的方式有：

- 通过面对面的提交，订户从注册机构接受载有证书和私钥的介质
- 按照湖北 CA 的提示，通过网络将证书下载到本地存放介质

完成以上行为表明订户已经接受证书。订户在接受到证书后，应立即对证书进行验证和测试。

3.5.4.2 湖北 CA 发布证书

湖北CA将订户已经接受的证书发布到允许公众访问的资料库中。对于订户明确表示拒绝发布证书信息的，湖北CA不发布该订户证书信息。

3.5.4.3 湖北 CA 通知其他实体关于证书的签发

湖北CA没有义务将证书签发信息通知除证书持有者、RA及业务受理点以外的实体。

3.5.5 密钥对和证书的使用

3.5.5.1 订户私钥和证书的使用

签名密钥对只用于签名与签名验证，加密密钥对只用于加密解密，两种密

钥对中的私钥使用符合证书中KeyUsage扩展的要求；证书的使用符合本CPS3.4节“证书的用途”的要求。若与订户有密钥对和证书使用协议的，则按照订户协议的要求使用。未按规定用途使用造成的损失由证书持有者自己承担。

订户必须在接受证书后，才能使用证书对应的私钥，并保护私钥免受未授权的使用。在证书到期或被撤销之后，订户必须停止使用私钥。

3.5.5.2 依赖方对公钥和证书的使用

依赖方依赖证书的前提是同意依赖方协议中的条款。依赖方必须根据环境和条件来判断，证书是否可依赖。

当依赖方接受到签名信息后，应该：

- 获得对应的证书及信任链
- 验证证书的有效性
- 确认该签名对应的证书是依赖方信任的证书
- 证书的用途适用于相应的签名
- 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。

当依赖方需要发生加密信息给接受方时，须先通过适当的途径获得接受方的加密证书，然后使用该证书上的公钥对信息加密，依赖方应将加密证书应同加密信息一同发送给接受方。

3.5.6 证书更新

3.5.6.1 证书更新的情况

当证书到期时，如果证书中的公钥和其他任何信息没有发生变化，订户可以通过证书更新来获得新的证书。过期的证书也可以进行更新。

证书更新期限为一年。可以根据实际的业务需要，与订户签定协议规定证书更新期限，最长不能超过五年，被撤消的证书不能进行证书更新。

3.5.6.2 请求证书更新的人

证书持有者本人或其授权代表可以请求证书更新。

3.5.6.3 处理证书更新请求

湖北CA在对证书持有者证书进行更新前：

申请对应的原证书存在并由湖北CA签发。

用原证书上的证书持有者公钥对申请的签名进行验证。

基于原注册信息，按照密钥更新时的要求，进行身份鉴别。

以上验证和鉴别通过后才可进行证书更新。

3.5.6.4 通知订户新证书签发

湖北CA签发新证书后，及时通知证书持有者其证书已被签发，常用的方式有：

- 面对面的方式
- 呼叫中心、传真、电子邮件方式
- 其他湖北CA 认为安全可行的方式

3.5.6.5 构成更新证书接受的行为

证书持有者接受更新证书的方式有：

- 通过面对面的提交，证书持有者从注册机构接受载有证书和私钥的介质
- 按照湖北 CA 的提示，通过网络将证书下载到本地存放介质

完成以上行为表明证书持有者已经接受证书，证书持有者在接受到证书后，应立即对证书进行验证和测试。

3.5.6.6 湖北 CA 对更新证书的发布

湖北CA将证书持有者已经接受的证书发布到允许公众访问的资料库中。对于证书持有者明确表示拒绝发布证书信息的，湖北CA不发布该证书持有者证书信息。

3.5.6.7 湖北 CA 通知其他实体证书的发布

湖北CA没有义务将证书签发信息通知除证书持有者、证书持有者和RA以外的实体。

3.5.7 证书密钥更换

3.5.7.1 证书密钥更换的情况

当证书到期、丢失、密钥发生泄漏或者其他需要更换密钥的时候，证书持有者可以通过证书密钥更换来获得一张包含新公钥但其他信息不变的新证书。

3.5.7.2 请求证书密钥更换的人

证书持有者本人或其授权代表可以请求证书密钥更换。

3.5.7.3 证书密钥更换请求的处理

湖北CA在对证书持有者证书进行密钥更换前，需要确认密钥更换请求是被更换证书的证书持有者（或证书持有者授权的代表）提出的，例如：要求证书持有者提交登记时候提供的鉴别信息（或者等同的方式），或要求密钥更换申请者提交原证书中公钥对应的私钥的签名。

用于原始证书申请的鉴别也可以用于处理密钥更换请求。

如果证书持有者证书对应的私钥发生泄露，湖北CA将采用初始证书申请的鉴别流程来处理密钥更换请求。

3.5.7.4 证书持有者新证书签发的通知

湖北CA签发证书后，及时通知证书持有者其证书已被签发，常用的方式有：

- 通过面对面的方式
- 邮政信函结合电子邮件方式
- 其他湖北CA 认为安全可行的方式

3.5.7.5 构成密钥更新证书接受的行为

证书持有者接受证书的方式有：

- 通过面对面的提交，证书持有者从注册机构接受载有证书和私钥的介质
- 按照湖北 CA 的提示，通过网络将证书下载到本地存放介质

完成以上行为表明证书持有者已经接受证书。证书持有者在接受到证书后，应立即对证书进行验证和测试。

3.5.7.6 湖北 CA 对密钥更新证书的发布

湖北CA将证书持有者已经接受的证书发布到允许公众访问的资料库中。对于证书持有者明确表示拒绝发布证书信息的，湖北CA不发布该证书持有者证书信息。

3.5.7.7 湖北 CA 通知其他实体证书的签发

湖北CA没有义务将证书签发信息通知除证书持有者、证书持有者和RA以外的实体。

3.5.8 证书变更

3.5.8.1 证书变更的情况

当证书中包含的信息（除公钥外）发生变化时，证书持有者可以通过证书

变更获得新证书。证书的变更将被视为初始的证书申请。

3.5.8.2 请求证书变更的人

下列人员可以提交证书申请：

- 能够独立承担民事责任的自然人或其授权代表
- 具有独立法人资格的机构的授权代表

3.5.8.3 证书变更请求的处理

湖北CA将对申请证书变更的证书持有者进行标识和身份鉴别，具体要求同初始身份验证相同。

3.5.8.4 证书持有者新证书签发的通知

湖北CA签发证书后，及时通知证书持有者其证书已被签发，常用的方式有：

- 通过面对面的方式
- 邮政信函结合电子邮件方式
- 其他湖北CA 认为安全可行的方式

3.5.8.5 构成变更证书接受的行为

证书持有者接受证书的方式有：

- 通过面对面的提交，证书持有者从注册机构接受载有证书和私钥的介质
- 按照湖北 CA 的提示，通过网络将证书下载到本地存放介质

完成以上行为表明证书持有者已经接受证书。证书持有者在接受到证书后，应立即对证书进行验证和测试。

3.5.8.6 湖北 CA 对变更证书的发布

湖北CA将证书持有者已经接受的证书发布到允许公众访问的资料库中。对

于证书持有者明确表示拒绝发布证书信息的，湖北CA不发布该证书持有者证书信息。

3.5.8.7 湖北 CA 通知其他实体证书的签发

湖北CA没有义务将证书签发信息通知除证书持有者、证书持有者和RA以外的实体。

3.5.9 证书撤销

3.5.9.1 撤销的情况

下列情况出现时，证书必须被撤销并发布在证书撤销列表中：

- 证书持有者或湖北CA有理由相信证书持有者证书对应的私钥出现了安全问题
- 湖北CA有理由相信或怀疑其证书对应的私钥出现了安全问题
- 有证据表明证书持有者违反了本CPS或证书持有者协议中的条款或相关法律法规
- 证书持有者协议终止
- 湖北CA相信证书中或者证书申请中的信息是错误的
- 证书持有者工作性质发生变化
- 证书持有者受到国家法律发规制裁
- 证书持有者没有或无法履行有关规定和义务
- 政务机构有理由相信或强烈怀疑其下属雇员的私钥安全已经受到损害
- 证书持有者请求撤消其证书
- 证书仅用于依赖主导的系统并由依赖方提出撤消申请的

3.5.9.2 请求证书撤销的人

请求证书撤销的人包括：

- 个人证书证书持有者或其授权代表

- 机构证书证书持有者的授权代表
- 设备证书证书持有者的授权代表
- 湖北CA的授权代表
- 证书使用唯一依赖方
- 司法机关等公共权力部门的授权代表

3.5.9.3 证书撤销请求的处理

在执行证书撤销前，湖北CA需要验证证书的撤销请求来自证书持有者或其授权代表。用于鉴别撤销请求的方式包括：

- 证书持有者提交登记时候提供的鉴别信息（或者等同的方式），如果证书持有者能够正确提交相关信息，证书撤销会自动执行
- 证书持有者使用原私钥对撤销请求进行数字签名

证书撤消后，湖北CA通过短信、电话、传真、电子邮件、邮政信函或者快递服务等方式告诉告诉证书持有者或依赖方证书撤消结果。

3.5.9.4 撤销请求的宽限期

证书撤销请求必须在发现需要撤销后24小时内向湖北CA提出。

3.5.9.5 湖北 CA 处理撤销请求的时间要求

湖北CA在24小时内，撤消符合条件的证书并发布到证书撤消列表。

3.5.9.6 依赖方进行撤销检查的要求

依赖方在信任证书前，必须对证书的状态进行检查，检查方式包括：查询最新的证书撤销列表、证书实体查询等。

湖北CA将在公司网站（WWW.HBCA.ORG.CN）上提供证书撤销列表、在线证书实体查询。

3.5.9.7 证书撤销列表签发频率

湖北CA将在4小时签发一次证书撤销列表。

湖北CA的根证书发生撤销时签发证书撤消列表。

3.5.9.8 证书撤销列表发布的最大滞后时间

证书撤销列表生成后，立刻发布。

3.5.9.9 在线撤销/状态检查的可用性

撤销信息或其他证书状态信息通过湖北CA公司网站上提供的服务在线获得，服务时间是7*24小时查询服务。

3.5.9.10 在线撤销检查的要求

依赖方是否检查证书撤消列表完全取决于应用的安全要求。很多的应用本身建有用户帐户数据库并基于用户帐户进行应用控制，证书在此只起身份鉴别的，在这种情况下检查证书是否撤消不一定是必须的。

对于安全保障要求高且完全依赖证书进行身份鉴别与授权的应用，依赖方在信任一个证书前必须通过证书状态在线查询检查该证书状态。

3.5.9.11 可获得撤销公告的其他方式

除了证书撤消列表、证书状态在线查询外，湖北CA如提供其他形式的撤消信息发布途径，将予以公布。

3.5.9.12 针对密钥泄露的特殊要求

湖北CA的私钥被泄露或者怀疑被泄露，我们将在24小时内发布在公司网站上，并通过可能的方式尽快通知所有参与方和潜在的证书依赖方。

3.5.10 证书状态服务

3.5.10.1 操作特征

证书状态可以通过湖北CA网站上查询，公布服务地址、服务接口等。

3.5.10.2 服务的可用性

证书状态服务保证7*24小时不间断的可用，不安排服务中断时间。

3.5.10.3 可选功能

在线证书状态查询是一项必须的服务。

3.5.11 密钥托管和恢复

3.5.11.1 密钥生成、备份和恢复的策略与实施

湖北CA的根密钥不能被托管。

证书持有者的签名密钥对由证书持有者的密码设备生存并由其保管，不能被托管。加密密钥对由国家密钥管理局规划建设的湖北省密钥管理中心提供，实行托管。

密钥恢复是指加密密钥对的恢复，密钥管理中心不负责签名密钥对的恢复。密钥恢复分为两类：

- 证书持有者密钥恢复；当证书持有者密钥损坏或丢失后，某些密文数据将无法还原，此是证书持有者可以申请密钥恢复，经湖北CA审核通过其申请后，将恢复证书持有者的密钥并下载到证书持有者的证书载体中。
- 问责取证密钥恢复；经湖北CA审核问责取证申请后，由密钥恢复模块恢复所需的密钥并记录于特定载体中。

第四章 应用集成支持服务操作规范

4.1 服务策略和流程

湖北 CA 的提供的服务内容有：

- 制定证书应用的管理策略和流程, 指导或参与业务系统证书应用部分的开发和实施
- 制定项目管理制度
- 制定安全控制流程, 明确人员职责
- 实施证书软件发布版本管理
- 项目开发程序和文档等资料归档保存

4.2 应用接口

湖北 CA 提供的应用接口规范：

- 密码设备接口包括服务器端底层应用接口和客户端证书介质的低层应用接口, 该两种接口均符合有关标准规范
- 通用密码服务接口是屏蔽了底层不同密码设备类型和底层接口的通用中间件, 主要包括服务器端组件接口和客户端控件接口, 该两种接口均支持不同 CA 公司所签发的符合国家标准的数字证书

4.3 集成内容

湖北 CA 依据双方协议,为应用单位提供证书应用接口程序集成工作,包括:

- 证书应用接口开发包
- 接口说明文档
- 证书应用接口开发培训和集成技术支持
- 协助应用系统开发商完成联调测试工作

第五章 信息服务操作规范

5.1 服务内容

5.1.1 证书信息服务

湖北 CA 可根据电子政务信息系统的需要,依据双方协议,将湖北 CA 系统中签发、更新的数字证书定时或实时与对方实现数据同步。

5.1.2 CRL 信息服务

湖北 CA 可以根据需要,将 CRL 实时发布到指定的电子政务信息系统中。

5.1.3 服务支持信息服务

湖北 CA 依据用户、应用系统集成商、应用系统的需要,发布包括 CPS、常见问题解答证书应用接口软件包等文挡、软件。

5.1.4 决策支持信息服务

湖北 CA 依据用户和依赖方需要,根据双方签定的协议,可以提供包括用户档案、投诉处理、客户满意度以及服务效率等信息。

5.2 服务管理规则

- 湖北 CA 内部员工,依据角色设定对应的信息访问权限,并对其操作进行记录。
- 用户单位的管理员对非授权信息的访问,需要制定单位内部管理规定进行管理。
- 问责程序需要进行信息访问时,湖北 CA 将严格审查问责人员身份和授

权文件,无误后方可进行问责举证。

- 湖北 CA 或用户单位的上级监管部门需要信息访问时,按照湖北 CA 信息管理规则提供信息访问权限。

5.3 服务方式

5.3.1 证书信息同步服务

湖北 CA 可以根据需要，通过采用 webservice 面向应用信息系统提供数字证书应用同步服务，同时在湖北 CA 与应用系统之间的通讯,采取添加数字签名方式,确保传输数据的完整性和机密性。

5.3.2 CRL 信息同步服务

湖北 CA 依据需要,可以为应用系统同步调用 CRL, 同时为 CRL 添加数字签名方式,确保 CRL 的有效性。

5.3.3 服务支持信息服务

面向用户发布如下信息：

- 湖北 CA 电子政务电子认证服务业务规则
- 客户服务流程及其相关费用
- 操作手册
- 常见问题解答
- 用户获取帮助的联系方式
- 根据协议约定的其他信息
- 湖北 CA 认为应该发布的其他信息

面向应用系统集成商发布如下信息:

- 数字证书应用接口软件包
- 数字证书应用接口实施指南
- 常见问题解答
- 用户获取帮助的联系方式

- 根据协议约定的其他信息
- 湖北 CA 认为应该发布的其他信息

面向应用系统发布如下信息:

- 时间戳服务数据接口
- Http 协议的 CRL 发布接口
- Ldap 协议的 CRL 发布接口
- Ldap 协议的证书发布接口
- Ocsp 服务接口

5.3.4 决策支持信息服务

湖北 CA 面向应用提供以下服务:

- 用户档案信息：分业务、地域、时段等提供用户信息的统计分析服务
- 投诉处理信息：分项目、时间、用户群、问题类别等提供汇总信息和分析
- 客户满意度信息：提供面向业务的客户满意度调查信息
- 服务效率信息：提供面向业务的服务效率分析信息

第六章 使用支持服务操作规范

6.1 服务内容

6.1.1 面向证书持有者的服务

6.1.1.1 数字证书管理

数字证书的导入、导出、客户端证书管理工具的安装、使用、卸载等。

6.1.1.2 数字证书应用

数字证书用于身份认证、电子签名、加解密等应用出现的证书无法读取、签名失败、证书验证失败等应用问题.

6.1.1.3 证书存储介质硬件设备使用

证书存储介质使用过程中出现的口令锁死、驱动安装、介质异常等.

6.1.1.4 电子政务电子认证服务支撑平台使用

平台应用问题:证书更新失败、下载异常、无法提交注销申请等.

6.1.2 面向应用提供方的服务

6.1.2.1 电子认证软件系统使用

提供受理点系统、注册中心系统、LDAP、OCSP、信息服务系统等系统的使用支持. 如证书信息无法查询、数据同步失败、服务无响应等.

6.1.2.2 电子签名服务中间件的应用

解决服务中间件的集成时出现的诸如客户端平台适应性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等。

6.2 服务方式

6.2.1 坐席服务

湖北 CA 设置有服务热线,热线坐席根据用户的问题请求,查询知识库系统,协助用户处理。

6.2.2 在线服务

- QQ 等实时通讯系统进行互动联系
- 远程终端协助帮助解决用户疑难
- 在线方式和传统模式的结合

6.2.3 现场服务

- 根据用户的需要,由技术工程师和客户服务人员上门为用户处理数字证书应用中存在的问题.

6.2.4 满意度调查

- 采取调查问卷通过电话、WEB 网站、邮件系统、短信平台、传真等多种用户可接受的方式不定期地开展用户满意调查,分析调查结果,改善服务.
- 将满意度调查过程中的相关文档全部归档保存.

6.2.5 投诉处理

- 通过电话、WEB 网站、邮件系统、短信平台、传真、QQ 类及时通讯工具等接受用户投诉,投诉受理过程中记录投诉问题, 及时将结果反馈给

用户.

- 将投诉受理过程中的相关文档全部归档保存.

6.2.6 培训

- 培训方式依照湖北 CA 与证书持有者或依赖方协议中双方约定的形式开展.
- 培训内容可以包括以下内容:电子政务电子认证服务基础性技术知识、客户服务规范、数字证书应用集成规范、常见问题解答、操作使用手册等.

6.3 服务质量

- 坐席服务、在线服务、现场服务时间做到充分满足各类用户的需要.服务时间是至少是 5 天*8 小时.
- 热线电话服务时间是 7 天*24 小时不间断服务.
- 技术问题和客服问题均按照问题类别、严重程度依次分类登记和处理,制定响应处理流程和工作机制,确保服务的及时性和连续性,各类响应时间按双方协议为准,或以不影响客户使用数字证书为准则.

第七章 安全保障规范

7.1 物理安全控制

7.1.1 场所位置和建筑

湖北CA的机房建设至少参照以下国家标准：

GB 50174-93：《电子计算机机房设计规范》

GB 2887-89：《计算站场地技术条件》

GB 9361-88：《计算站场地安全要求》

湖北CA的所有操作均在受到物理保护的环境下进行。所采取的物理保护手段能够阻止、防止并检测未经授权的使用、访问或者披露敏感的信息和系统。

存放湖北CA设备的建筑，建立了多级的物理安全防护体系，为不同的区域设置不同的安全级别，实施不同程度的物理安全防护措施。每个人员只能进入其被授权访问的物理区域。

7.1.2 物理访问

根据业务功能划分为公共区、服务区、管理区、核心区，各功能区对应的安全级别为控制区、限制区、敏感区、机密区，安全级别和要求逐步提高。

当人员需要从一个区域进入另一个区域或者安全级别较高的区域的时候，必须通过相应的访问控制。

只有授权人员才能对湖北CA的物理设备进行操作，针对不同安全级别的物理设备提供不同程度的访问控制措施，包括但不限于以下方法：

- 授权人员需使用授权口令登录物理设备
- 确保设备访问日志不被篡改并且定期检查
- 需要至少两个具有操作权限的人员来操作密码模块或者计算机系统
- 对高安全级别的物理设备进行 24 小时自动监视

机房的所有门都足够的坚实，能够防止非法进入。机房设置门禁和入侵报警系统来重点保护机房物理安全。

7.1.3 电力和空调

湖北CA的安全设施设有主、备电力供应系统，在单路电源损坏时，自动切换,维系正常运转，同时采取不间断电源(UPS)来保证供电的稳定性和可靠性，不间断电源可持续提供4小时的电能供应。机房所有区域均设有空调，对于关键的安全设施，也设有主、备空调系统来控制温度和湿度，供配电系统布线采用金属管、硬质塑料管、塑料线槽等。

7.1.4 防水措施

湖北CA的安全设施安装在具有防水设备的场所，并制定相应的流程，以防止洪水或者其他由于暴露在有水的环境对系统造成损害，发现水害能及时报警。

7.1.5 火灾预防与保护

湖北CA的设备机房提供了火灾自动报警系统和应急处理装置，并符合GB 50116-98：《火灾自动报警系统设计规范》的要求。

办公区域、机房均设置火灾自动报警系统和灭火系统，火灾报警系统包括火灾自动探测、区域报警器和控制器等，能够对火灾发生区域以声、光或电的方式发出报警信号，并能以手动或自动方式启动灭火设备。

7.1.6 介质存储

湖北CA保证存储介质不会被意外破坏（如：水，火和电磁干扰），不被进行未授权的物理访问（被修改、信息泄露未授权等）。完整记录介质的使用、库存、维修、销毁事件等。

7.1.7 废物处理

湖北CA制定废物处理流程，对不再使用的敏感介质、文件和其他废物，以安全的方式销毁，销毁方法包括但不限于以下形式：

- 纸质的敏感信息需要通过粉碎、焚烧或其它不可恢复的方法处理

- 废弃的密码设备需要根据制造商的指南将其物理销毁或者格式化

7.1.8 异地备份

湖北CA提供进行安全异地备份的设施，所备份的业务数据进行异地保存。

7.1.9 入侵侦测报警系统

安装入侵检测报警系统，发生非法入侵能及时报警。

7.2 操作过程控制

7.2.1 可信角色

担当可信角色的人员是可信人员。可信人员是指能够访问、进入或者控制认证或密钥操作的人员。湖北CA的员工、第三方服务人员和顾问等是被认定为可信的人员。成为可信人员必须符合本CPS中关于人员的要求。

要求做到以下控制：

- 资格、经历和无过失要求；
- 背景审查程序；
- 培训和再培训；
- 工作轮换周期和频率；
- 独立合约人的控制；
- 各种文档的控制。

7.2.2 每项任务需要的人数

湖北CA建立、维护和执行严格的控制流程，基于工作要求和工作安排建立职责分割措施，确保由可信人员共同完成敏感操作。敏感的内部控制流程要求至少有两名可信人员参与设备的逻辑访问和物理访问。对湖北CA的硬件密钥设备的生命周期（从设备开始服役到逻辑/物理销毁）过程中的访问，必须严格的要求多名可信人员共同参与。一旦一个密码模块被激活，进一步的逻辑或物理

访问必须实施职责分割。掌握设备的物理权限的人员不能再持有分享秘密，反之亦然。

7.2.3 每个角色的标识和鉴别

对于所有将要成为可信角色的人员，在执行下述操作前，湖北CA将对其身份进行鉴别：

- 赋予可信角色可访问的设施的权限
- 为其发放电子凭证，用于访问特定的信息系统和电子政务电子认证服务系统

身份的鉴别包括：人事部门的可信人员对被调查人的身份进行当面的核查，并要求被审查人提供有效身份证件。湖北CA保留更进一步的背景调查权利。

7.2.4 需要职责分割的角色

湖北CA内部以下任何两个或两个以上角色，不能由同一个人员担当，进行职责分割。必须进行职责分割的角色包括但不限于：

业务受理录入岗位、审核岗位互相分割；

CA(RA)系统审计岗位和运维 人员岗位互相分割；

客户资料管理岗位，客户服务岗位互相分割；

机构信息上报岗位，客户资料管理岗位互相分割；

密钥管理岗位，CA 系统操作岗位互相分割；

运维人员和服务人员分割；

安全管理人员和运维人员分割的原则。

7.3 人员控制

7.3.1 资历和安全要求

湖北CA将要求可信人员，提供有关教育背景、工作资格以及相关从业经历

的证明。对于重要角色，需要具备资格、经历和无过失要求。

7.3.2 背景审查流程

湖北CA制定了并执行严格的背景审查流程，对担当可信角色和重要岗位的人员进行调查，并定期进行复审。背景调查中，有下列行为的被审查人不能通过审查：

- 被审查人提供虚假信息
- 有犯罪记录
- 有不良财务记录

7.3.3 培训要求

湖北CA将对其人员进行培训，每年对关键岗位的人员培训不得少于40学时。培训内容与人员对应职责相关，包括：使用、操作和维护电子政务电子认证服务系统过程中涉及的职责、安全机制（例如：灾难恢复的方法、业务连续性要求）以及电子政务电子认证服务系统的软硬件操作规范等。

湖北CA将定期对培训内容进行审查。

7.3.4 再培训周期和要求

湖北CA将定期对相关人员进行再培训。

7.3.5 岗位轮换的频率和顺序

湖北CA依据人员、业务条件，每年不定期地在相关部门之间以及部门内部之间进行岗位轮换。每次岗位轮换周期不底于一个季度。

7.3.6 未授权行为的处罚

湖北CA建立、维护和实施一套管理办法，对相关人员的未授权行为（如：对电子政务电子认证服务系统和资料库等进行的未授权访问）进行管理，根据未授权行为出现的次数和严重性进行处罚。

7.3.7 独立合约人的要求

当满足如下条件时，湖北CA可以允许独立合约人或者顾问成为可信人员：

- 没有合适的雇员能够担当这个可信角色
- 对于担当可信角色的独立合约人或者顾问与雇员具有同等的信任

另外，需要访问湖北CA的安全设施的独立合约人和顾问，必须由可信人员的护送和直接监督。

7.3.8 提供给员工的文档

为保障湖北CA运营的规范和安全，湖北CA将为所有员工提供的文档包括：岗位职责、业务操作说明和湖北CA安全管理的相关规范等。

7.4 审计流程

7.4.1 被记录事件的类型

湖北 CA 将对可审计的事件类型进行记录。所有的日志，无论是电子生成或者是手工生成，都必须包括事件的数据和时间，引发事件实体的身份。

可审计的事件类型包括：

- CA、RA、KMC 系统运行日志、密钥管理执行和数据备份情况；
- 鉴别验证、客户资料、客户满意度、投诉处理、支持的证书认证操作规程是否与公司 CPS 表达一致等；
- 财务基本数据；
- 可信人员管理及操作事件；
- IT 重要资产；
- 不符合规程的事件的记录

7.4.2 处理日志的周期

湖北CA对日志进行定期检查，以便发现重要的安全和操作事件。

7.4.3 审计日志的保存期限

审计日志在被处理后，应在本地保存不得少于两个月。

7.4.4 审计日志的保护

湖北CA制定相关流程，确保审计日志不被未授权的访问、复制、修改和删除。

7.4.5 审计日志的备份

审计日志依据相关管理办法定期进行备份。

7.4.6 脆弱性评估

通过对日志中记录的事件进行审查，对系统的脆弱性进行评估。这种评估不定期执行。

7.5 记录归档

7.5.1 归档的记录类型

湖北CA至少需要归档以下记录：

- 所有在 7.4 节涉及的审计数据
- 证书申请的相关信息
- 证书生命周期的相关信息

7.5.2 归档记录的保存期限

信息保存期为证书失效后十年。

7.5.3 归档记录的保护

湖北CA采取安全措施，保证未授权的用户不会浏览、修改和删除电子政务

电子认证服务机构的归档记录。

7.5.4 归档记录的备份流程

湖北CA将对电子和纸质归档记录定期进行异地备份,同时,重要数据资料分别由两人保留归档数据的两个拷贝。

7.5.5 归档记录的时间戳要求

湖北CA的归档记录将包含记录产生的时间和日期信息。

7.5.6 归档记录收集系统（内部或外部）

归档记录由各部门按年度统一归到办公室管理。

7.5.7 获得和检验归档记录的流程

只有被授权的可信人员能够访问归档记录。所有记录被访问后，需对两个归档拷贝进行比较,验证其完整性。

7.6 湖北 CA 根密钥的更替

湖北CA根密钥更新时,采取与系统根密钥初始化生成相同的流程和方法,新旧密钥过渡期间,采用新私钥为旧公钥签名证书、旧私钥为新公钥签名证书、新私钥为新公钥签名证书方式,保证用户和依赖方能够可靠地验证湖北CA机构根证书以及确保证书信任

湖北CA根密钥的更替，将上报电子政务电子认证服务管理部门，并在其监督下进行重新生成新的密钥，并将自签名证书上交电子政务电子认证服务管理部门备案。

7.7 事故和灾难恢复

7.7.1 事故处理流程

湖北CA针对事故的性质制定和实施灾难恢复流程。重大事故立即上报电子政务电子认证服务管理部门。

7.7.2 计算资源、软件和/或数据遭到破坏

湖北CA的计算资源、软件或数据等遭到破坏后，湖北CA将采取相应的业务恢复措施。

7.7.3 湖北 CA 私钥的泄露处理流程

一旦湖北CA的密钥泄露需要被撤销，并将立即上报电子政务电子认证服务管理部门，并尽可能地通知潜在的依赖方。

7.7.4 灾难发生后的业务连续性

湖北 CA 定制了包括恢复应用、数据、硬件、通讯和其它 IT 基础设施《湖北 CA 事故灾难管理办法》，明确 CA 系统（包括应用、数据）发生灾难后的业务恢复时间是 24 小时，硬件、通讯（湖北 CA 可控制部分）和其他 IT 基础设施发生灾难后的业务恢复时间是 48 小时。制定业务连续性计划，并经常进行检查和更新，对灾难恢复流程进行演练，定期检察设备等。

7.8 电子政务电子认证服务的终止

湖北CA拟暂停或者终止认证服务时，将在暂停或终止认证服务六十个工作日前，选定业务承接方，就业务承接事项作出妥善安排，并在暂停或终止认证服务四十五个工作日前向国家工业和信息化部、国家密码管理局报告。若湖北CA不能就业务承接事项作出妥善安排，将在暂停或终止认证服务六十个工作日前，向国家工业和信息化部、国家密码管理局提出安排其他电子政务电子认证

服务机构承接业务的申请。

7.9 技术安全控制

7.9.1 密钥对的生成和安装

7.9.1.1 湖北 CA 根密钥对的生成

由湖北 CA 密钥管理员按照湖北 CA 的密钥生成规程产生湖北 CA 根密钥对。

湖北 CA 密钥生成规程规定了 CA 密钥产生的流程控制及参加人员。湖北 CA 用于签发证书和证书状态信息的密钥对由国家密码主管部门批准和许可的硬件设备生成。密钥生成后已经上报电子政务电子认证服务管理部门，并在其监督下进行生成新的密钥，并将自签名证书上交电子政务电子认证服务管理部门备案。

7.9.1.2 证书持有者密钥的生成

证书持有者的密钥对可以由证书持有者或者湖北CA生成，由湖北CA生成的证书持有者密钥的传递符合下节的要求

7.9.1.3 传递交私钥给证书持有者

证书持有者的加密私钥是在KMC 产生的，该私钥只保存在KMC 和证书持有者介质。

在加密私钥从 KMC 到证书持有者的传递过程中采用国家密码管理局许可的对称密钥算法加密。湖北 CA 无法获得，保证了证书持有者的密钥安全。

如果证书持有者自己生成密钥对，则不需要传递私钥。

如果是湖北CA代表证书持有者生成私钥，将通过双方协商的安全方式进行保管和传递给证书持有者，也会采取合理的方式确保私钥在未被证书持有者接受前不能被激活。

7.9.1.4 传送公钥给证书签发机构

证书持有者的签名证书公钥通过安全通道，经注册机构传递到湖北 CA。

证书持有者的加密证书公钥，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，采用国家密码管理局许可的通讯协议及密钥算法，保证了传输中数据的安全。

7.9.1.5 传送湖北 CA 公钥给依赖方

对于湖北 CA 的根 CA 公钥，通过如下方式传输给依赖方：

- 依赖方访问湖北 CA 的证书网站上下载湖北 CA 根证书
- 湖北 CA、注册机构或其合作伙伴到依赖方业务系统现场将 CA 证书安装到业务系统中
- 湖北 CA、注册机构或其合作伙伴通过签名电子邮件将 CA 证书传输给依赖方湖北 CA、注册机构或其合作伙伴分发给依赖方的软件中绑定、包含有湖北 CA 根证书

7.9.1.6 密钥长度

湖北CA证书持有者的密钥对至少使用1024比特的RSA密钥或者同等安全程度的密钥。

7.9.1.7 公钥参数的生成和资格检查

符合国家密码管理部门的要求，加密公钥采用的是 KMC 自动生成，签名公钥采用的是在 USBkey 里自动生成，根证书加密和签名公钥均是由加密机自动生成。

7.9.1.8 密钥用途

在湖北 CA 证书服务体系中的密钥用途和证书类型紧密相关,包括但不限于如下：

- 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

- 加密密钥用于信息加密和解密

7.9.2 私钥保护和密码模块的工程控制

密码模块标准和控制：

- 证书持有者可以按照相关协议要求选用密码模块，并妥善保管私钥。
- 湖北CA所使用的密码模块，通过了国家密码主管部门的专门检测。

私钥多人控制： 湖北CA系统根私钥的生成、更新、注销、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5张管理员卡中，只有其中三至五人在场并许可的情况下，才能对私钥进行上述操作。

私钥托管：湖北CA的私钥和证书持有者的签名私钥不能托管。

私钥备份：湖北CA 对CA 私钥通过专门的备份IC卡进行备份。KMC 备份托管加密私钥，确保加密私钥的安全。

湖北CA私钥的备份：湖北CA私钥的备份由多人控制，并放置在安全的场所。

证书持有者私钥备份：湖北CA 建议证书持有者对私钥进行备份，并对备份的私钥采用口令或其他访问控制机制保护，防止非授权的修改或泄露。

私钥归档：湖北CA 对到期后的证书持有者私钥归档保存至少5 年，湖北CA 的密钥管理策略和流程阻止归档CA 密钥对返回到产品系统中。归档私钥到期后，湖北CA 将按规定流程销毁。

私钥导入或导出密码模块：湖北CA 的CA 密钥对在硬件密码模块上生成，保存和使用。湖北CA 制定了相关的密钥管理策略来有效防止了CA 私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

保存在密码模块的私钥：湖北CA 私钥以加密的形式存放在硬件密码模块中，在密码模块中使用。

激活私钥的方法：湖北CA 私钥激活按多人控制进行分割。

当证书持有者私钥存放在证书持有者计算机的软件密码模块中时，证书持有者应该采用合理的措施从物理上保护计算机以防止在没有得到证书持有者授

权的情况下其他人员使用证书持有者的计算机。如果存放在软件密码模块中的私钥没有口令保护，那么，软件密码模块的加载意味着私钥的激活。如果该私钥有口令保护，软件密码模块加载后，还需要输入口令才能激活私钥。

当证书持有者私钥存放在诸如USB Key等硬件密码模块中，这时私钥可以通过PIN 码（口令）等安全机制保护。如果私钥没有PIN码（口令）或指纹鉴别保护，那么，当用户计算机上安装了相应的硬件密码模块驱动程序后，将USB Key 或智能卡插入到相应的读卡设备中，私钥将会被激活可以使用。如果私钥有PIN 码（口令）保护，那么，当用户计算机上安装了相应的驱动程序并将USB Key 或智能卡插入到相应的读卡设备中后，只有输入PIN 码（口令），私钥才被激活可以使用。私钥一旦激活，将是长期的。

解除私钥激活状态的方法：湖北CA的私钥在激活后就持续有效，断电将自动解除激活状态。证书持有者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、移开令牌和自动锁定等。

销毁私钥的方法：具有销毁密钥权限的管理员使用含有自己的身份的加密IC卡管理程序，进行销毁密钥的操作，需要三名管理员同时在场。

加密模块定级：由国家密码管理部门负责。

7.9.3 密钥对管理的其它方面

公钥归档：对于生命周期外的CA和最终证书持有者证书，湖北CA 将进行归档，归档的证书存放在归档数据库中。

证书操作期和密钥对使用期限：

- 签名用途的证书，私钥期限不超过证书有效期，公钥可以超过证书有效期。
- 加密用途的证书，公钥期限不超过证书有效期，私钥可以超过证书有效期。
- 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。
- 对于证书持有者证书，有效期最长不超过5年。对于湖北CA的证书，最长的有效期不超过50年。

7.9.4 激活数据

激活数据的产生和安装：湖北CA 私钥的激活数据由硬件加密卡内部产生，并分割保存在5 个IC 卡中，需通过专门的读卡设备和软件读取。证书持有者激活数据是私钥保护口令。湖北CA 提供唯一的不可猜测的证书私钥口令。这些私钥口令由湖北CA 根据授权和操作的许可实施批准并且仅发放给授权证书持有者。

激活数据的保护：保存有湖北CA 私钥的激活数据的5 个IC 卡分别依据湖北CA 职责分割的要求由湖北CA 5个不同的可信人员掌管。证书持有者的激活数据是私钥保护密码，如果证书证书持有者使用口令或PIN 码保护私钥，证书持有者应妥善保管好其口令或PIN 码，防止泄露或窃取。如果证书证书持有者使用生物特征保护私钥，证书持有者也应注意防止其生物特征被人非法获取。

激活数据的其它方面:湖北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消后，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。私钥归档的操作按照本CPS的规定处理。证书持有者的私钥不再被使用，或者与私钥相对应的公钥到期或者被撤消后，由证书持有者决定其销毁方法，证书持有者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，证书持有者必须按照本CPS 的规定执行。

7.9.5 计算机安全控制

特定的计算机安全技术要求：湖北CA 的数字证书签发系统的数据文件和设备由专职管理员维护管理，未经授权，其它人员不能操作和控制湖北CA 系统；其它普通用户无系统账号和密码，密码口令的设置符合安全管理要求。湖北CA将使用防火墙、入侵检测系统以及防病毒软件系统来保护产品网络免受内部和外部的入侵并限制网络活动的性质和来源。湖北CA在逻辑上与其他组件的系统和信息访问进行隔离，这种分离只允许已经定义的应用进程进行访问。

计算机安全等级:湖北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家密码管理局的审核，湖北CA 数字证书认证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。湖北CA的计算机安全等级不低于三级。

生命周期技术控制

系统开发控制：湖北 CA 的系统的开发由满足国家相关安全和密码标准的可靠软件开发商完成。

安全管理控制：湖北 CA 采取有效的安全管理控制机制来控制和监控 CA 系统配置以防止未授权的修改。

7.9.6 生命周期的安全控制

湖北 CA 和相关产品开发商以及标准机构共同合作，根据国际安全标准和发展动态，在不影响正常提供服务的前提下，积极采用国内外先进的技术和设备，及时进行技术更新。湖北 CA 对系统的任何修改和升级会记录在案并予以控制。

- CA 系统运行管理

CA 系统的操作流程需要文档化并进行维护；

CA 系统变更需要经运营安全策略委员会批准；

可能对系统的安全性有影响的改动必须事先进行风险评估，改动前进行备份并得到运营安全策略委员会的授权；

测试系统、运营系统、网络设施具有专门的操作维护人员，并有相应的授权；

运维人员每季度定期检查网络稳定性、安全性及容量；

建立检测和防护控制防止病毒；

建立监控流程；

建立制度。

- CA 系统的访问管理

制定 CA 系统的访问管理；

制定 CA 系统访问人员角色职能定义及权限划分，明确授权；

制定网络安全策略；

制定操作系统及 CA 软件的安全访问策略；

建立各种对 CA 系统访问的审计措施。

- CA 系统的开发和维护

  操作系统软件升级时，应用系统软件需要重新测试；

  在 CA 系统中，购买或使用的软件需要严格检查是否有“木马”等危害性。

7.9.7 网络的安全控制

采取防火墙、病毒防治、入侵检测、漏洞扫描、数据备份、灾难恢复、安全身份认证等安全防护措施，湖北制定有关网络安全策略与实施方案，确保湖北CA认证系统网络安全。

第八章 法律责任相关要求

8.1 费用

8.1.1 收费项目和不收费项目

湖北 CA 根据双方签定的服务合同，约定开户费、服务费和更新费。

湖北 CA 暂不收取证书查询费用。

免费提供证书撤消和撤消列表（CRL）查询。

湖北 CA 有可能根据需要将在线查询（OCSP）服务作为增值服务收取费用。

8.1.2 退款策略

一旦证书持有者接受数字证书，湖北 CA 将不办理退款手续。

证书持有者接受数字证书后，由于湖北 CA 造成下列情况将退款：

- 合同无法履行
- 证书持有者的数字证书无法使用

8.2 财务责任

8.2.1 保险范围

湖北CA根据用户数量储存一定比例的准备金，具备承担对证书持有者、依赖方等造成的责任风险的能力,保证其具有维持其运作和履行其责任的财务能力,并依据本CPS规定，进行赔偿担保。

8.3 业务信息保密

8.3.1 保密信息范围

湖北 CA 的保密信息包括但不限于：

- 系统方面

认证系统结构、配置，包括系统、网络、数据库等；

认证系统安全策略和方案；

系统操作、维护记录；

各类系统操作口令。

- 运营管理方面

物理安全策略与实施方案，包括场地、访问控制、入侵检测等实施方案；

密钥管理策略与操作记录；

CA 或 RA 批准或拒绝的申请纪录；

可信人员名单；

运营安全管理策略和管理制度。

- 客户信息

客户的注册信息，包括电子和各类申请表等纸质材料；

客户系统、应用访问 CRL、OCSP 的记录（时间、频度）；

客户与认证机构、注册机构签订的协议；

8.3.2 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、申请操作指南等信息是公开

的。湖北CA在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。

证书持有者数字证书的相关信息可以通过湖北CA 目录服务等方式向外公布。

湖北CA 在其目录服务器中公布证书的撤消信息，供网上查询。

8.3.3 保护保密信息的责任

湖北 CA 不但有各种严格的管理制定、流程和技术手段保护自身的商业秘密，并且把保护客户信息作为自己应尽的义务。湖北 CA 的每个员工都要接受信息保密方面的培训。

8.4 个人隐私保密

8.4.1 隐私保密方案

除非证书申请人主动提供，湖北CA保证不会截取任何证书申请人的资料。

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

8.4.2 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。

8.4.3 不被视为隐私的信息

不被认为是隐私信息包括，要出现在证书中的信息，证书及证书状态。

8.4.4 保护隐私的责任

除非执法、司法方面的强制需要，湖北 CA 及其注册机构在没有获得客户授权的情况下，不会将客户隐私信息透露给第三方。有司法要求提供信息访问的需要按照下面的流程办理。

验证司法人员工作程序：

- 利用权威第三方提供的身份证明，也可以是政府机构发放的合法性文件（如：居民身份证）来证明证书持有者的身份；
- 通过电话、邮政信函或与此类似的其他方式确认个人信息的真实性；
- 通过可靠的方式确保证信息访问人员所在的组织、部门与证件中所列的组织、部门一致，确实被雇佣。

8.4.5 使用隐私信息的告知与同意

湖北 CA 或其注册机构如果需要将客户隐私信息用于双方约定的用途以外的目的，则需要事先告知客户并获得客户同意和授权，用户同意和授权信息以下列方式之一传送给湖北 CA 或其注册机构：

- 有手写签名的同意和授权文件，并将文件邮寄、快递到湖北 CA 或其注册机构;
- 将手写签名的同意和授权文件传真到湖北 CA;
- 以签名电子邮件的形式同意并授权。

8.4.6 依法律或行政程序的信息披露

由于法律执行、法律授权的行政执行的需要，湖北 CA 及其注册机构有可能需要将有关信息在客户知晓或不知晓的情况下提供有关执法机关、行政执行机关，即使出现这种情形，湖北 CA 及其注册机构也将尽可能地保护客户隐私信息。

8.4.7 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。

8.5 知识产权

除非额外声明，湖北CA 享有并保留对证书以及湖北CA 提供的全部软件的一切知识产权，包括所有权、名称权和利益分享权等。湖北CA 有权决定关联机构采用的软件系统，选择采取的形式、方法、时间、过程和模型，以保证系统

的兼容和互通。

按本CPS 的规定，所有由湖北CA 签发的证书和提供的软件中使用、体现和相关的一切版权、商标和其他知识产权均属于湖北CA 所有，这些知识产权包括所有相关的文件和使用手册。注册机构应征得湖北CA 的同意使用相关的文件和手册，并有责任和义务提出修改意见。

8.6 陈述与担保

除非湖北 CA 作出特别约定，若本认证业务规则的规定与湖北 CA 制定的其他相关规定、指导方针相互抵触，用户必须接受本认证业务规则的约束。在湖北 CA 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规则的规定执行；对协议中不同于本认证业务规则内容的约定，按双方协议中约定的内容执行。

8.6.1 电子政务电子认证服务机构的陈述与担保

湖北 CA 在提供电子政务电子认证服务活动过程中的承诺如下：

- 湖北 CA 遵守《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》和《电子政务电子认证服务管理办法》等相关法律法规，接受国家工信部和国家密码局的业务监督和指导，对湖北 CA 所签发的数字证书承担相应的责任和义务。
- 湖北 CA 保证使用的系统及密码符合国家政策与标准，保证湖北 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。
- 湖北 CA 签发给证书持有者的证书符合湖北 CA CPS 规定的所有实质性要求。
- 湖北 CA 保证证书在有效期内的有效性和可靠性，将向证书证书持有者通报任何已知的、可能在本质上影响证书的有效性和可靠性事件。
- 湖北 CA 将及时撤消证书，并发布到 CRL 上供证书持有者查询。
- 证书公开发布后，湖北 CA 向证书依赖方保证，除未经鉴证的证书持有者信息外，证书中的其他证书持有者信息均为准确的。

8.6.2 注册机构的陈述与担保

湖北 CA 的注册机构和下层分支机构在参与电子政务电子认证服务过程中的承诺如下：

- 严格执行湖北 CA 中心制定的证书管理和发放策略，服从湖北 CA 整体的管理和规范要求；提供给证书证书持有者的注册过程完全符合湖北 CA CPS 的所有实质性要求。
- 在湖北 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。
- 及时响应并向湖北 CA 提交证书持有者证书申请、撤消、更新等服务请求。

8.6.3 证书持有者的陈述与担保

订户一旦接受湖北 CA 签发的证书，就被视为向湖北 CA、注册机构及证书依赖方的有关当事人作出以下承诺：

- 订户已阅读并理解本 CPS 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。
- 订户在证书申请表上填列的所有声明和信息必须是完整、真实和准确的，并可供湖北 CA 或注册机构检查和核实。
- 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。
- 订户对使用私钥的行为负责。
- 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，订户应立刻通知湖北 CA 和注册机构，及时申请采取证书撤消等业务处理。
- 订户已知其证书被冒用、破解或被他人非法使用时，应按湖北 CA CPS 的相关条款及时申请办理撤消其证书业务。

8.6.4 依赖方的陈述与担保

证书依赖方必须熟悉本 CPS 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。

依赖方在信赖其他证书持有者的数字证书前，必须采取合理步骤，查证证书持有者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理解本 CPS 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。

8.7 担保免责

湖北 CA 不对其签发的证书适用于其规定的目的以外的任何应用承担任何担保，对证书在其规定的目的以外的应用不承担任何责任。对由不可抗力，如战争、地震、洪灾、爆炸、恐怖活动等，造成的服务中断并由此造成的客户损失，湖北 CA 及注册机构不承担责任。

湖北 CA 在签发数字证书之前，证书申请者已同意遵守责任书或双方协议中的各项规定。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，得到了湖北 CA 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，湖北 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。湖北 CA 也不承担任何其他未经授权的人或组织以湖北 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。

8.8 有限责任

对于由于湖北 CA 自身原因，如没有严格按业务流程进行证书审批导致证书的错误签发、假冒，或管理上的疏忽导致 CA 私钥泄漏、盗用等，造成了证书证书持有者、依赖方的损失，湖北 CA 将承担相应的赔偿责任，但这种责任是有限的。

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

8.9 赔偿

赔偿的条件:

- 湖北 CA 在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发；
- 由于湖北 CA 的原因，使得证书中出现了错误信息；
- 由于湖北 CA CA 私钥的泄漏；
- 当湖北 CA 终止或暂停认证服务时，因湖北 CA 未就业务承接有关事项作出妥善安排而导致给证书持有者造成损失时。

在如下情况，证书持有者因自身原因造成湖北 CA、依赖方损失应当承担责任:

- 证书持有者在证书申请中对事实做虚假或错误描述；
- 在证书申请中证书持有者没有披露重要的事实，如果这种错误表述或遗漏是因为粗心或故意欺骗任何一方；
- 证书持有者没有使用可信系统保护私钥，或者没有采取必要的注意防止证书持有者私钥的安全损害、丢失、泄漏、修改或非授权的使用；
- 证书持有者使用的名字（包括但不限于通用名、域名和 e-mail 地址）破坏了第三方的知识产权法。

在如下情况，依赖方对自身原因造成的湖北 CA 损失承担责任：

- 依赖方没有执行依赖方职责义务；
- 依赖方在不合理的环境下信赖一个证书；
- 依赖方没有检查证书状态确定证书是否过期或撤消。

赔偿的限制：

- 湖北 CA 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年服务费的拾倍。
- 湖北 CA 只有在湖北 CA 证书有效期限内承担损失赔偿。

赔偿流程：

- 由客服部提出具体赔偿申请；
- 安全部进行审核；
- 总经理批准或公司运营安全策略委员批准
- 财务部进行财务审核；
- 返回给客服部执行。

8.10 有效期限与终止

8.10.1 有效期限

湖北 CA 的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， 有效期限为 2 年，当出现提前终止的情况，湖北 CA 将会公布终止的原因。

8.10.2 终止

当新版本的《湖北CA电子政务电子认证服务业务规则》正式发布生效时，旧版本的《湖北CA电子政务电子认证服务业务规则》自动终止。

8.10.3 效力的终止与保留

湖北 CA 的本 CPS 中止（而非更新），意味着湖北 CA 电子认证业务的终止。湖北 CA 中止电子认证业务的过程将按国家有关主管部门的规定进行，并根据规定对受影响的客户进行安排，保证客户的利益不受影响或将受影响的程度减少到最小。

当由于某种原因，如内容修改、与适用法律相冲突，CPS 和其他相关协议中的某些条款失效后，不影响文件中其他条款的法律效力。

8.11 对参与者的个别通告与沟通

湖北 CA 及其注册机构在必要的情况下，如在主动撤消证书持有者证书、发现证书持有者将证书用于规定外用途及证书持有者其他违反证书持有者协议的行为时，会通过适当方式，如电话、电邮、信函、传真等，个别通知证书持有者、依赖方。

8.12 修订

8.12.1 修订程序

本CPS将尽量避免不必要的修改。但不定期地，湖北CA 将对本CPS 进行检查、评估，当湖北CA 认为应该对本CPS 做出修改时，湖北CA 运营安全策略委员会成员将对本CPS 及其他相关文档、协议提出修改建议，获得湖北CA 运营安全策略委员会批准后，由指定人员负责组织有关文档、文件的修改。修改后的CPS 及其他相关文档报运营安全策略委员会批准后正式发布。

8.12.2 通知机制和期限

本 CPS 在湖北 CA 的网站上发布。版本更新时，最新版本的《湖北 CA 电子政务电子认证服务业务规则》会在湖北 CA 的网站及时公布，对具体个人和单位证书持有者不再另行通知。

8.12.3 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CPS 。

8.13 争议处理

如果湖北CA、证书持有者和依赖方之间出现争议时，有关方面可依据协议通过协商解决，协商解决不了的，可通过法律解决。

8.14 管辖法律

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

8.15 与适用法律的符合性

湖北 CA 的所有业务、活动、合同、协议符合中华人民共和国法律、法规，包括但不限于公司法、合同法、隐私法、消费者权益保证法等。

8.16 一般条款

8.16.1 完整协议

本CPS 将替代提供电子政务电子认证服务过程中已经发生、与主题相关的书面或口头解释。

8.16.2 转让

湖北 CA、注册机构、证书持有者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。

8.16.3 分割性

当法庭或其他仲裁机构判定协议中的某一条款由于某种原因无效或不具执行力时，不会出现因为某一条款的无效导致整个协议无效。

8.16.4 强制执行

在湖北 CA、注册机构、证书持有者和依赖方之间出现纠纷、诉讼时，胜讼方可以要求对方支付有关诉讼费作为对其补偿的一部分。免除一方对某次合同违约的赔偿不意味着免除对其他合同违约的赔偿。

8.16.5 不可抗力

当由于不可抗力，如地震、洪灾、雷电等自然灾害和战争等，造成湖北CA、注册机构无法提供正常的服务时，湖北CA、注册机构不承担由此给客户造成的损失。