湖北省数字证书认证管理中心有限公司

电子认证业务规则

版本 3.0

湖北省数字证书认证管理中心有限公司

2022 年 8 月

目录

1. 概括性描述 10

1.1 概述 10

1.2 文档名称与标识 10

1.3 电子认证活动参与者 11

1.3.1 电子认证服务机构（CA） 11

1.3.2 注册机构（RA） 11

1.3.3 受理点 11

1.3.4 订户 11

1.3.5 依赖方 12

1.3.6 其他参与者 12

1.4 证书应用 12

1.4.1 适合的证书应用 12

1.4.2 限制的证书应用 13

1.5 策略管理 13

1.5.1 策略文档管理机构 13

1.5.2 联系信息 13

1.5.3 决定 CPS 符合策略的机构 14

1.5.4 CPS 批准程序 14

1.6 定义和缩写 14

2. 信息发布与信息管理 15

2.1 认证信息的发布 15

2.2 发布的时间或频率 15

2.3 信息库访问控制 16

3. 身份的标识与鉴别 16

3.1 命名 16

3.1.1 名称类型 16

3.1.2 对名称意义化的要求 16

3.1.3 订户的匿名或伪名 17

3.1.4 理解不同名称形式的规则 17

3.1.5 名称的唯一性 17

3.1.6 商标的识别、鉴别和角色 18

3.2 初始身份确认 18

3.2.1 证明拥有私钥的方法.....18
3.2.2 组织机构身份的鉴别.....18
3.2.3 个人身份的鉴别.....19
3.2.4 场景证书订户身份的鉴别.....19
3.2.5 协同证书订户身份的鉴别.....19
3.2.6 没有验证的订户信息.....19
3.2.7 授权确认.....19
3.3 密钥更新请求的标识与鉴别.....19
3.3.1 常规密钥更新的标识与鉴别.....20
3.3.2 吊销后密钥更新的标识与鉴别.....20
3.4 吊销请求的标识与鉴别.....20
4. 证书生命周期操作要求.....20
4.1 证书申请.....20
4.1.1 证书申请实体.....20
4.1.2 注册过程与责任.....21
4.2 证书申请处理.....21
4.2.1 执行识别与鉴别功能.....21
4.2.2 证书申请批准和拒绝.....21
4.2.3 处理证书申请的时间.....22
4.3 证书签发.....22
4.3.1 证书签发中 RA 和 CA 的行为.....22
4.3.2 CA 和 RA 对订户的通告.....22
4.4 证书接受.....23
4.4.1 构成接受证书的行为.....23
4.4.2 CA 对证书的发布.....23
4.4.3 CA 在颁发证书时对其他实体的通告.....23
4.5 密钥对和证书的使用.....23
4.5.1 订户私钥和证书的使用.....24
4.5.2 依赖方公钥和证书的使用.....24
4.6 证书更新.....25
4.6.1 证书更新的情形.....25
4.6.2 请求证书更新的实体.....25
4.6.3 证书更新请求的处理.....25
4.6.4 颁发新证书时对订户的通告.....25
4.6.5 构成接受更新证书的行为.....25

4.6.6 CA 更新证书的发布 25
4.6.7 CA 在颁发证书时对其他实体的通告 26
4.7 证书密钥更新 26
4.7.1 证书密钥更新的情形 26
4.7.2 请求证书密钥更新的实体 26
4.7.3 证书密钥更新请求的处理 26
4.7.4 颁发新证书时对订户的通告 26
4.7.5 构成接受密钥更新证书的行为 26
4.7.6 CA 对密钥更新证书的发布 27
4.7.7 CA 对其他实体的通告 27
4.8 证书变更 27
4.8.1 证书变更的情形 27
4.8.2 请求证书变更的实体 27
4.8.3 证书变更请求的处理 27
4.8.4 颁发新证书时对订户的通告 27
4.8.5 构成接受变更证书的行为 27
4.8.6 CA 对变更证书的发布 28
4.8.7 CA 对其他实体的通告 28
4.9 证书吊销和挂起 28
4.9.1 证书吊销的情形 28
4.9.2 请求证书吊销的实体 29
4.9.3 吊销请求的流程 29
4.9.4 吊销请求宽限期 29
4.9.5 CA 处理吊销请求的时限 29
4.9.6 依赖方检查证书吊销的要求 29
4.9.7 CRL 发布频率 29
4.9.8 CRL 发布的最大滞后时间 29
4.9.9 在线状态查询的可用性 30
4.9.10 在线状态查询要求 30
4.9.11 吊销信息的其他发布形式 30
4.9.12 密钥损害的特别要求 30
4.9.13 证书挂起的情形 30
4.9.14 请求证书挂起的实体 31
4.9.15 证书挂起和恢复（解挂）的流程 31
4.9.16 挂起的期限限制 31
4.10 证书状态服务 31

4.10.1 操作特征.....31
4.10.2 服务可用性.....31
4.10.3 可选特征.....31
4.11 订购结束.....31
4.12 密钥生成、备份与恢复.....32
4.12.1 密钥生成、备份与恢复的策略与行为.....32
4.12.2 会话密钥的封装与恢复的策略与行为.....32
5. 认证机构设施、管理和操作控制.....33
5.1 物理控制.....33
5.1.1 场地位置与建筑.....33
5.1.2 物理访问.....33
5.1.3 电力与空调.....34
5.1.4 水患防治.....34
5.1.5 火灾防护.....34
5.1.6 介质存储.....34
5.1.7 废物处理.....34
5.1.8 异地备份.....35
5.2 程序控制.....35
5.2.1 可信角色.....35
5.2.2 每项任务需要的人数.....35
5.2.3 每个角色的识别与鉴别.....36
5.2.4 需要职责分割的角色.....36
5.3 人员控制.....36
5.3.1 资格、经历和无过失要求.....36
5.3.2 背景审查程序.....36
5.3.3 培训要求.....37
5.3.4 再培训周期和要求.....37
5.3.5 工作岗位轮换周期和顺序.....37
5.3.6 未授权行为的处罚.....37
5.3.7 独立合约人的要求.....38
5.3.8 提供给员工的文档.....38
5.4 审计日志程序.....38
5.4.1 记录事件的类型.....38
5.4.2 处理日志的周期.....38
5.4.3 审计日志的保存期限.....38

5.4.4 审计日志的保护.....39
5.4.5 审计日志备份程序.....39
5.4.6 审计收集系统.....39
5.4.7 对导致事件实体的通告.....39
5.4.8 脆弱性评估.....39
5.5 记录归档.....39
5.5.1 归档记录的类型.....39
5.5.2 归档记录的保存期限.....39
5.5.3 归档文件的保护.....40
5.5.4 归档文件的备份程序.....40
5.5.5 记录时间要求.....40
5.5.6 归档收集系统.....40
5.5.7 获得和检验归档信息的程序.....40
5.6 电子认证服务机构密钥更替.....40
5.7 损害与灾难恢复.....41
5.7.1 事故和损害处理程序.....41
5.7.2 计算机资源、软件和/或数据的损坏.....41
5.7.3 实体私钥损害处理程序.....41
5.7.4 灾难后的业务连续性能力.....41
5.8 CA 或 RA 的终止.....42
6. 认证系统技术安全控制.....42
6.1 密钥对的生成和安装.....42
6.1.1 密钥对的生成.....42
6.1.2 私钥传送给订户.....43
6.1.3 公钥传送给证书签发机构.....43
6.1.4 CA 公钥传送给依赖方.....43
6.1.5 密钥的长度.....43
6.1.6 公钥参数的生成和质量检查.....43
6.1.7 密钥使用目的.....44
6.2 私钥保护和密码模块工程控制.....44
6.2.1 密码模块的标准和控制.....44
6.2.2 私钥多人控制.....44
6.2.3 私钥托管.....45
6.2.4 私钥备份.....45
6.2.5 私钥归档.....45

6.2.6 私钥导入、导出密码模块.....45
6.2.7 私钥在密码模块的存储.....45
6.2.8 激活私钥的方法.....46
6.2.9 解除私钥激活状态的方法.....46
6.2.10 销毁私钥的方法.....47
6.2.11 密码模块的评估.....47
6.3 密钥对管理的其他方面.....47
6.3.1 公钥归档.....47
6.3.2 证书操作期和密钥对使用期限.....47
6.4 激活数据.....48
6.4.1 激活数据的产生与安装.....48
6.4.2 激活数据的保护.....48
6.4.3 激活数据的销毁.....48
6.4.4 激活数据的其他方面.....48
6.5 计算机安全控制.....49
6.5.1 特别的计算机安全技术要求.....49
6.5.2 计算机安全评估.....49
6.6 生命周期技术控制.....49
6.6.1 系统开发控制.....49
6.6.2 安全管理控制.....49
6.6.3 生命期的安全控制.....49
6.7 网络的安全控制.....50
7. 证书、证书吊销列表和在线证书状态协议.....50
7.1 证书.....50
7.1.1 版本号.....50
7.1.2 证书扩展项及其关键性.....50
7.1.3 算法对象标识符.....51
7.1.4 名称形式.....51
7.2 证书吊销列表.....51
7.2.1 版本号.....51
7.2.2 CRL 和 CRL 条目扩展项.....51
7.3 在线证书状态协议.....52
7.3.1 版本号.....52
7.3.2 OCSP 扩展项.....52
8. 认证机构审计和其他评估.....52

8.1 评估的频率或情形 52
8.2 评估者的资质 52
8.3 评估者与被评估者之间的关系 53
8.4 评估内容 53
8.5 对问题与不足采取的措施 53
8.6 评估结果的传达与发布 53
9. 法律责任和其他业务条款 54
9.1 费用 54
9.1.1 证书签发和更新费用 54
9.1.2 证书查询费用 54
9.1.3 证书吊销或状态信息的查询费用 54
9.1.4 其他服务费用 54
9.1.5 退款策略 54
9.2 财务责任 55
9.2.1 保险范围 55
9.2.2 对最终实体的保险或担保 55
9.3 业务信息保密 55
9.3.1 保密信息范围 55
9.3.2 不属于保密的信息 56
9.3.3 保护保密信息的责任 56
9.4 个人隐私保密 56
9.4.1 隐私保密方案 56
9.4.2 作为隐私处理的信息 56
9.4.3 不被视为隐私的信息 56
9.4.4 保护隐私的责任 56
9.4.5 使用隐私信息的告知与同意 57
9.4.6 依法律或行政程序的信息披露 57
9.4.7 其他信息披露情形 57
9.5 知识产权 57
9.6 陈述与担保 58
9.6.1 电子认证服务机构的陈述与担保 58
9.6.2 注册机构的陈述与担保 58
9.6.3 订户的陈述与担保 59
9.6.4 依赖方的陈述与担保 59
9.6.5 其他参与者的陈述与担保 60

9.7 担保免责 60
9.8 有限责任 61
9.9 赔偿 61
9.10 有效期限与终止 62
9.10.1 有效期限 62
9.10.2 终止 62
9.10.3 效力的终止与保留 62
9.11 对参与者的个别通告与沟通 62
9.12 修订 62
9.12.1 修订程序 62
9.12.2 通知机制和期限 63
9.12.3 必须修改业务规则的情形 63
9.13 争议处理 63
9.14 管辖法律 63
9.15 与适用法律的符合性 63
9.16 一般条款 64
9.16.1 完整协议 64
9.16.2 转让 64
9.16.3 分割性 64
9.16.4 强制执行 64
9.16.5 不可抗力 64
9.16.6 其他条款 65

1. 概括性描述

1.1 概述

湖北省数字证书认证管理中心有限公司（HuBei Digital Certificate Authority Center Co.,Ltd）简称为“HBCA”或“湖北 CA” 。HBCA 是经国家相关部门批准成立的专业化的第三方电子认证服务机构。湖北 CA 严格依照《中华人民共和国电子签名法》、《电子认证服务管理办法》的要求以及相关管理规定，向公众（包括政府机构、企事业单位和个人）提供数字证书申请、颁发、存档、查询、更新、废止等服务，并通过以 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、企业信息化的发展构建安全可靠的信任环境。

HBCA 电子认证业务规则（CPS）的编写遵从《中华人民共和国电子签名法》、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》、中华人民共和国工业和信息化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）》以及 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）。本 CPS 详细阐述了 HBCA 在实际工作和运营中所遵循的各项规范。本 CPS 作为实际应用和操作的文件依据，适用于所有与 HBCA 有关的电子认证活动参与者。作为公告，向社会公布 HBCA 关于证书服务的基本立场和观点。与 HBCA 有关的电子认证活动参与者，必须完整地理解和执行 HBCA 电子认证业务规则所规定的条款，承担相应的责任和义务。本 CPS 为通用版本，若 HBCA 发布的其它业务 CPS 有特别约定的以相应业务 CPS 为准。

1.2 文档名称与标识

本文档名称为《湖北省数字证书认证管理中心有限公司电子认证业务规则》。

《湖北 CA 电子认证业务规则》、《湖北 CA CPS》、《HBCA CPS》等类似名称或表述均应被视为对本文档的引用。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构（CA）

HBCA 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证书的权威机构，是颁发数字证书的实体。

1.3.2 注册机构（RA）

注册机构 RA（Registration Authority）负责订户证书的申请受理、审批和管理，直接面向证书订户，并负责在订户和 CA 之间传递证书管理信息。

HBCA 可以授权下属机构或者委托外部机构作为注册机构，负责提供证书业务办理、身份鉴证与审核等服务。

HBCA 授权外部机构作为注册机构，应在与外部机构签署的协议中，明确双方的权力和义务，以及承担的法律责任。

1.3.3 受理点

受理点是受理证书业务的服务实体。作为 HBCA 认证服务体系架构内直接面向用户的服务主体，经过 CA 或 RA 的授权从事相应证书服务。

HBCA 或 RA 授权外部机构作为受理点，应在与外部机构签署的协议中，明确双方的权力和义务，以及承担的法律责任。

1.3.4 订户

订户是指向 HBCA 申请证书的实体。

需要明确的是，证书订户与证书主体是两个不同的概念。“证书订户”是指向 HBCA 申请证书的实体，通常为个人或机构；“证书主体”是指与证书信息绑定的实体，服务器证书中的“证书主体”通常是指受信任的服务器或用于确保与某一机构安全通信的其它设施。证书订户需要承担相应的责任与义务，而证书主体则是证书所要证明的可信赖方。

1.3.5 依赖方

依赖方即指依据本 CPS 合理的信任证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方应合理的信任证书以及相关的数字签名。如果信任数字签名时需要额外保证，依赖方应在得到这些保证后合理的信任该数字签名。

1.3.6 其他参与者

其他参与者指上述未提及的为 HBCA 证书认证服务体系提供或参与相关服务的其他实体。

1.4 证书应用

1.4.1 适合的证书应用

HBCA 签发的数字证书的应用范围包括电子商务及其他社会信息化应用等领域，为建设互联网络的信任环境开展基础性服务。具体请参阅 https://www.hbca.org.cn。

HBCA 签发的数字证书主要包括个人证书、机构证书、设备证书、场景证书、协同证书等。订户可以根据自己的应用需要自行选择合适的证书类型。具体如下表：

证书类型	适合的证书应用
个人证书	1、自然人在网络环境下标识个人身份、执行电子签名或数据加密。 2、机构雇员在网络环境下标识个人身份及其代表的机构岗位或职责，执行电子签名或数据加密。
机构证书	机构或法人在网络环境下标识证书所载主体的身份，执行电子签名或数据加密。
设备证书	在网络环境下标识证书所载设备（包括网络设备、系统、服务器等网络通信实体）的身份，实现对设备的身份认证以及数据传输的机密性和完整性。
场景证书	场景证书是一种适用于对即时业务或者特定场景业务进行签名认证的数字证书。
协同证书	协同证书是一种适用于证明订户在移动化和云服务环境中所进行

	的身份认证与电子签名的数字证书。

另外，特别说明的是，测试证书及其签名均不具备法律效力，其是在测试系统、非生产环境中作测试使用，不可应用在正式生产环境中。

1.4.2 限制的证书应用

因在以下场景下使用所造成的损失和法律后果由订户自己承担。

1、任何违反国家法律、法规或破环国家安全的情形。

2、用于危险环境中的控制设备，或用于要求防失败的场合，因为它的任何故障都可能导致死亡、人员伤害或严重的环境破坏。

3、任何未经 HBCA 认可的应用系统。

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 的管理机构是 HBCA 安全策略委员会，由 HBCA 安全策略委员会负责本 CPS 的制定、发布、更新等事宜。

1.5.2 联系信息

HBCA 将对认证业务规则进行严格的版本控制，并由 HBCA 负责解释,如有疑问请与安全策略委员会联系。

电　　话：400-870-8080

地　　址：湖北省武汉市武昌区中南路街道民主二路 75 号华中小龟山金融文化公园 9 栋

邮政编码：430000

网站地址：https://www.hbca.org.cn

电子邮件：cps@hbca.org.cn

1.5.3 决定 CPS 符合策略的机构

决定 HBCA CPS 符合策略的机构为湖北省数字证书认证管理中心有限公司安全策略委员会。

1.5.4 CPS 批准程序

本《电子认证业务规则》由安全策略管理委员会，组织 CPS 编写小组。编写小组完成编写 CPS 草案后，将 CPS 评审稿提交安全策略管理委员会审批。经审批通过后，在 HBCA 的网站上对外公布。

本《电子认证业务规则》经安全策略管理委员会审批通过后，从对外公布之日起三十日之内向工业和信息化部备案。

本 CPS 的发布不对其他实体单独通知。

1.6 定义和缩写

下列定义适用于本 CPS。

电子认证服务机构（CA）：即 Certificate Authority，或 Certifying Authority，是指签发数字证书的可信第三方权威机构。

注册机构（RA）：Registration Authority，注册机构是受理数字证书的申请、更新、变更和吊销等业务的实体。

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

证书吊销列表（CRL）：Certificate Revocation List，一个定期（或根据要求）发布的、并由 CA 机构数字签名的信息列表，内容通常包含被吊销证书的序列号、签发者、签发日期等。用来识别被吊销的证书。也被称为数字证书黑名单、数字证书废止列表等类似名称。

在线证书状态协议（OCSP）：Online Certificate Status Protocal。为依赖方提供实时查询证书状态信息的协议。

电子签名认证证书（数字证书）：Digital Certificate，是经一个权威的、可信赖

的、公正的第三方电子认证服务机构签发的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展项信息的电子文档。

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

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

私钥（电子签名制作数据）：非对称密码算法中只能由拥有者使用的不公开的密钥。

公钥（电子签名验证数据）：非对称密码算法中可以公开的密钥。

2. 信息发布与信息管理

2.1 认证信息的发布

HBCA 通过目录服务（LDAP）发布订户的证书和 CRL，通过 OCSP 提供证书状态查询服务。用户可以通过访问 HBCA 的目录服务器获取证书的信息和证书吊销列表（CRL），通过在线证书状态查询协议（OCSP） 查询证书状态。或应订户和依赖方的需要采用其他方式提供证书的发布或查询服务。

本 CPS 发布到 HBCA 的网站上，供相关方下载、查询。

2.2 发布的时间或频率

HBCA 电子认证业务规则一经发布、更改，即时生效，并对一切仍有效的数字证书的使用者、新的数字证书及相关的电子认证活动参与者均具备约束力。对具体个人或机构不另行通知。

证书在签发后，HBCA 将通过目录服务器或其它指定途径自动发布该证书。

HBCA 通常在 24 小时内自动发布最新 CRL。

2.3信息库访问控制

对于公开发布的证书、CRL、CPS 等公开信息，HBCA 允许公众自行通过网站查询和访问。

HBCA 通过网络安全防护、安全管理制度确保这些信息只有经授权的人员才能更新。

3. 身份的标识与鉴别

3.1命名

3.1.1 名称类型

HBCA 根据对应实体的类型不同，通过甄别名（Distinguished Name，简称 DN）来唯一标识证书主体的身份信息。

HBCA 证书符合 X.509 标准，甄别名格式遵守 X.500 标准。

3.1.2 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公钥绑定的实体信息。

机构证书的甄别名通常包含机构名称或机构的证件号码，作为标识订户的关键信息被认证。

个人证书的甄别名通常可包含个人的真实名称或者证件号码，作为标识订户的关键信息被认证。

设备证书的甄别名通常包含订户所拥有的域名、IP 或设备标识，结合该订户的其他信息一起被鉴别和认证。

场景证书的甄别名通常包含业务场景的相关数据信息，包括但不限于业务场景中的实体名称信息、实体标识信息以及其他场景信息。

协同证书的甄别名参照机构和个人证书的相关要求。

3.1.3 订户的匿名或伪名

HBCA 不接受或者不允许任何匿名或者伪名，仅接受有明确意义的名称作为唯一标识符。

3.1.4 理解不同名称形式的规则

最终订户证书的主题域中包含一个 X.500 甄别名，格式如下:

属　性	值
C - Country（国家）	CN
O - Organization（机构）	.证书订户所在机构的机构名或不用
OU - Organizational Unit（机构部门）	.订户组织机构部门或证书主体其它标识或不用
S - State（省）	.订户所在省或不用
L - Locality（位置）	.订户所在地或不用
CN - Common Name（通用名）	这个属性包括但不限于： .个人姓名（与身份证上标明的一致） .组织机构名或机构标识（与机构的证件号码一致） .域名或 IP（与域名证书或有关证明上标明的一致）
E（E-mail 地址）	.订户证书中包含的 E-mail 地址

3.1.5 名称的唯一性

HBCA 签发给某个实体的证书，其主题甄别名，在 HBCA 信任域内是唯一的，其中的例外包括签发双证书时（一个签名证书、一个加密证书），属于同一实体的两个证书具有同样的主题甄别名,但证书的密钥用法扩展项不同。当出现相同的名称时，以先申请者优先使用，后申请者在唯一标识名称后面加识别码予以区别。

3.1.6 商标的识别、鉴别和角色

HBCA 不受理采用商标作为名称标识的订户申请。HBCA 签发的证书的主题甄别名中将不包含商标名。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

HBCA 通过使用经数字签名的 PKCS#10 格式的证书请求，或其他相当的密码格式，或其他 HBCA 批准的方法，验证证书申请者拥有私钥。

如果 HBCA 代表订户产生一个密钥对（如订户接受 HBCA 交付的存有证书及对应私钥的密码模块时，视为订户拥有私钥），那么这个要求不适用。

3.2.2 组织机构身份的鉴别

对于组织机构订户，HBCA或授权的注册机构需要鉴别：

1、订户提交的组织身份信息。鉴别方法包括核对订户提交的组织有效身份证件或证件的具体信息。必要时可以通过权威第三方数据库对身份证件信息进行比对。组织有效身份证件指政府部门签发的证件或文件，包括但不限于营业执照、事业单位登记证、社会团体登记证、政府批文等。

2、组织授予经办人的授权证明。鉴别方法包括但不限于检查组织或组织的法定代表人授权给经办人办理证书事宜的授权文件或授权条款。

3、经办人的个人身份证明材料。

4、如该组织需申请服务器类型的证书，需域名使用权证明材料。例如要求提交域名所有权文件、归属权证明文件或者申请者对所有权的书面承诺等。

鉴别方式可以采用面对面现场鉴别或远程鉴别。当HBCA或授权的注册机构认为有需要时，可以增加其他方式，包括但不限于鉴别组织的法定代表人身份或要求经办人提交法定代表人有效身份证件证明。

HBCA保留根据最新国家政策法规的要求更新组织身份鉴别方法与流程的权利。

3.2.3 个人身份的鉴别

对于个人订户，HBCA或授权的注册机构将验证个人有效身份证件或证件的具体信息，核实个人订户身份的真实性。个人有效身份证件指政府部门签发的证件，包括但不限于：身份证、港澳台居民居住证、户口簿、护照、军官证等。

鉴别方式可以采用面对面现场鉴别或远程鉴别。必要时，可以通过权威第三方数据库信息比对、手机短信验证等其他可靠的方式鉴别。

HBCA保留根据最新国家政策法规的要求更新个人身份鉴别方法与流程的权利。

3.2.4 场景证书订户身份的鉴别

场景证书订户身份的鉴别参照机构或个人身份鉴别方法进行鉴别，也可以采取包括录音、录像、可信数据源等有效的身份核验方式进行自动鉴别。

3.2.5 协同证书订户身份的鉴别

协同证书订户身份的鉴别参照机构或个人身份鉴别方法进行鉴别，也可以采取包括录音、录像、可信数据源等有效的身份核验方式进行自动鉴别。

3.2.6 没有验证的订户信息

订户提交鉴证文件以外的信息为没有验证的订户信息。

3.2.7 授权确认

为确保经办人具有特定的许可，能够代表组织机构获取数字证书，需要组织机构对其授权。组织机构在 HBCA 的数字证书申请表及委托授权书上加盖单位公章后，则证明本组织对经办人的授权确认。

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，HBCA 可以决定该有效期的长短。签名密钥到期后必须更新（重新产生一组公钥和私钥密钥对），加密密钥在保证安全的前提下可根

据订户要求或证书应用的需要保持原有密钥对不更新，并向发证机构申请重新签发证书。

当订户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。

当国家主管部门对密钥的管理、更新等有规定的，HBCA 将严格予以执行。

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，HBCA 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

HBCA 对吊销后的证书不进行密钥更新。

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《电子认证业务规则》 所规定的义务，由 HBCA 和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

证书申请的实体可以是任何个人、机构或其它客观存在的实体，其本人或机构的合法授权经办人或实体拥有者都可以为该实体提交证书申请。证书申请者提交的信息必须真实，否则后果由证书申请者承担。

4.1.2 注册过程与责任

证书申请者按照本《电子认证业务规则》所规定的要求，通过现场面对面或在线方式提交证书申请，包括相关的身份证明材料。HBCA 或注册机构依据身份鉴别规范对证书申请者的身份进行鉴别，并决定是否受理申请。

订户：通过 HBCA 官方网站（https://www.hbca.org.cn）或者前往 HBCA 授权受理点领取数字证书申请表，根据申请表上的注意事项认真、如实、完整地填写申请表内容，并签名（个人）或盖章（单位）。配合 HBCA 或授权的注册机构完成对身份信息的采集、记录和审核。

HBCA：HBCA 参照 3.2 的要求对订户的身份信息进行采集、记录，审核。通过鉴证后，HBCA 向订户签发证书。

注册机构：授权的注册机构参照 3.2 的要求对订户的身份信息进行采集、记录和审核。通过鉴证后，注册机构向 HBCA 提交证书申请，由 HBCA 向订户签发证书。注册机构须接受 HBCA 的监督管理和审计。授权的注册机构应当按照 HBCA 的要求，向 HBCA 提交身份鉴证资料。

证书申请者应当提供真实、完整和准确的信息。如证书申请者未向 HBCA 提供真实、完整和准确的信息，或者有其他过错，给 HBCA 或电子签名依赖方造成损失的，由证书申请者承担赔偿责任。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

HBCA 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者的身份进行识别与鉴别。具体的鉴别流程详见 3.2 初始身份确认。

4.2.2 证书申请批准和拒绝

在 HBCA 或授权的注册机构收到申请者的申请后，按照本《电子认证业务规则》所规定的流程对申请信息及身份资料进行鉴别，根据鉴别结果决定批准或拒绝证书申请。

如果证书申请者通过本《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，HBCA 或授权的注册机构将批准证书申请，为证书申请者制作并颁发数字证书。

证书申请者未能通过身份鉴证，HBCA 或授权的注册机构将拒绝申请者的证书申请，并通知申请人鉴证失败，同时告知申请者鉴证失败的原因（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

在申请者提交资料齐全且符合要求的情况下，HBCA 或者授权的注册机构将在 3 个工作日内处理证书申请，如有特殊情况，可适当延长证书处理时间，但最长不超过 5 个工作日。HBCA 或授权的注册机构能否在上述时间期限内处理证书申请取决于证书申请者是否真实、完整、准确地提交了相关信息和是否及时地响应了 HBCA 的管理要求。

场景证书的申请为即时处理。

4.3 证书签发

4.3.1 证书签发中 RA 和 CA 的行为

在证书签发前 RA 管理员负责证书申请的鉴证，在证书申请通过鉴证后，RA 管理员将批准证书请求。为了批准证书申请，RA 管理员将使用证书登录到 RA 系统，查询系统记录的有关请求并批准请求。批准的信息将会发送到 HBCA 的 CA 系统，CA 系统签发证书并返回给 RA 系统供证书申请者下载。

4.3.2 CA 和 RA 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：

1、通过面对面的方式，通知订户到注册机构领取数字证书；注册机构把密码和证书等直接交付给订户，以通知订户证书信息已经正确生成；

2、电子或纸质回执、电子邮件通知订户；

3、其他 HBCA 认为安全可行的方式通知订户。

对于场景证书，订户成功完成电子签名，即视为证书签发成功，HBCA 不再就证书签发向订户进行其他方式的通告。

对于协同证书，通过系统提示、发送短信或电子邮件等方式对订户进行通告。

4.4 证书接受

4.4.1 构成接受证书的行为

通用证书签发完成后，HBCA 及其注册机构将数字证书当面或通过邮寄的方式给订户，订户自获得该数字证书起，就被视为同意接受数字证书；如果订户通过访问 HBCA 在线业务系统，进行证书下载，经系统提示证书下载成功后就同样被视为同意接受数字证书。

场景证书签发完成后，将证书应用于对应的电子签名时起，就被视为申请者同意接受证书。

对于协同证书，订户在收到 HBCA 证书签发成功的系统提示、短信或邮件信息后，视为同意接受证书。

4.4.2 CA 对证书的发布

HBCA 在证书签发完成后，将数字证书发布到目录服务器中，供订户和依赖方查询和下载。

场景证书通过电子签名的数据电文进行发布。

HBCA 根据与依赖方的约定，可向依赖方提供协同证书查询服务。

4.4.3 CA 在颁发证书时对其他实体的通告

对于签发的证书，HBCA 及注册机构不对其他实体进行通告。

4.5 密钥对和证书的使用

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

4.5.1 订户私钥和证书的使用

订户在提交了证书申请并接受了 HBCA 所签发的证书后，均视为已经同意遵守与HBCA、依赖方有关的权利和义务的条款。订户接收到数字证书，应妥善保存其证书对应的私钥。

通用证书订户接收到数字证书，应妥善保存其证书对应的私钥。

场景证书仅应用于订户对应的电子签名行为，订户只能在该次电子签名中使用私钥和证书。私钥将在完成本次电子签名数学运算后进行销毁，之后订户须停止使用该证书及对应的私钥。

协同证书订户必须使用其终端和云平台协同配合才能完成一次电子签名。私钥在终端和云平台协同运算生成的，订户必须通过协同运算才能使用私钥进行签名；私钥在云平台生成的，订户必须通过安全授权认证才能使用私钥进行签名。通过以上两种方式保证私钥仅由订户持有与控制。

订户只能在指定的应用范围内使用私钥和证书，订户只有在接收到相关证书之后才能使用对应的私钥，并且在证书到期或被吊销之后，订户必须停止使用该证书对应的私钥。

4.5.2 依赖方公钥和证书的使用

依赖方只能在恰当的应用范围内依赖于证书，并且与证书要求相一致（如密钥用途扩展等）。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方信任的证书；

3、检验证书的有效期，确认该证书在有效期之内；

4、查询证书状态，确认该证书没有被注销；

5、证书的用途适用于对应的签名或加密；

6、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，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密。

4.6 证书更新

4.6.1 证书更新的情形

为保证证书及其密钥对的安全有效，HBCA 会为签发的证书设置有效期，一般为一年。

场景证书不涉及证书更新业务。

4.6.2 请求证书更新的实体

任何合法持有有效期限内的HBCA证书的订户均可向HBCA申请更新持有的证书。

4.6.3 证书更新请求的处理

证书更新时，订户可以用原有的私钥对更新请求进行签名，HBCA 将会对用户的签名和公钥、更新请求内包含的用户信息进行正确性、合法性和唯一性的验证和鉴别。订户也可以选择初始证书申请流程进行证书更新，提交相应的证书申请和身份证明资料。当证书持有者的证书有效期到期前，HBCA 将通过短信提示、弹窗提示或者其它方式向证书订户发送证书更新提示。订户应当在证书有效期到期前，前往注册机构、受理点办理证书更新。由于订户未及时办理证书更新而导致原证书过期和无法使用，HBCA 及授权的注册机构、受理点不承担任何责任。

4.6.4 颁发新证书时对订户的通告

同 CPS § 4.3.2。

4.6.5 构成接受更新证书的行为

同 CPS § 4.4.1。

4.6.6 CA 更新证书的发布

同 CPS § 4.4.2。

4.6.7 CA 在颁发证书时对其他实体的通告

同 CPS § 4.4.3。

4.7 证书密钥更新

证书密钥更新即产生新的密钥对，使用与原证书一样的主题甄别名并由同一签发者签发新证书。

4.7.1 证书密钥更新的情形

当订户或其它参与者因如下原因需要生成一对新密钥并申请为新公钥签发一个新证书，可以选择证书密钥更新服务。

1、证书的有效期将要到期，证书更新；

2、证书密钥对已经或怀疑被泄露、被窃取、被篡改或者其它原因导致的密钥对安全性无法得到保证；

3、其他。

注：证书吊销后不允许证书密钥更新，场景证书不涉及证书密钥更新。

4.7.2 请求证书密钥更新的实体

同 CPS § 4.6.2。

4.7.3 证书密钥更新请求的处理

同 CPS § 4.6.3。

4.7.4 颁发新证书时对订户的通告

同 CPS § 4.6.4。

4.7.5 构成接受密钥更新证书的行为

同 CPS § 4.6.5。

4.7.6 CA 对密钥更新证书的发布

同 CPS § 4.6.6。

4.7.7 CA 对其他实体的通告

同 CPS § 4.6.7。

4.8 证书变更

在证书有效期内，当订户信息发生变化时，订户应进行证书变更，申请签发新的证书。HBCA 在对申请者递交的资料进行鉴别确认后，将为其重新签发证书。

4.8.1 证书变更的情形

证书变更指改变证书中订户信息而签发新证书的情形。当订户实体身份信息发生改变，而影响证书项内容时，证书订户有义务向 HBCA 报告并申请证书变更，将原证书吊销后重新签发新证书。

场景证书不涉及证书变更。

4.8.2 请求证书变更的实体

同 CPS § 4.6.2。

4.8.3 证书变更请求的处理

同CPS § 4.6.3。

4.8.4 颁发新证书时对订户的通告

同 CPS § 4.3.2。

4.8.5 构成接受变更证书的行为

同 CPS § 4.4.1。

4.8.6 CA 对变更证书的发布

同 CPS § 4.4.2。

4.8.7 CA 对其他实体的通告

同 CPS § 4.4.3。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

证书吊销分为主动吊销和被动吊销，主动吊销是指订户主动申请吊销其数字证书，注册机构审核申请后吊销其证书。被动吊销是指电子认证服务机构确认用户违反本《电子认证业务规则》申请、使用证书，或者证书主体消亡，则吊销数字证书。

一、发生下列情形之一的，订户应当主动申请吊销数字证书：

1、数字证书私钥被泄漏、被窃取、被篡改或者其它原因可能影响私钥安全的；

2、数字证书中的信息发生变更；

3、数字证书中的相关内容和申请时提交申请材料不一致；

4、认为本人不能履行或违反了本《电子认证业务规则》、其它协议、法规或法律所规定的责任和义务。

二、发生下列情形之一的，HBCA 可以强制吊销其签发的数字证书：

1、订户提供的信息不真实、不准确、不完整的；

2、订户没有履行本《电子认证业务规则》、其它协议、法规或法律所规定的责任和义务；

3、发现并证实其证书没有根据本《电子认证业务规则》要求的程序而签发的；

4、数字证书的安全性得不到保证；

5、法律、行政法规规定的其他情形。

三、HBCA 没有义务一定要公开某一张证书被吊销的原因。

四、场景证书不涉及证书吊销。

4.9.2 请求证书吊销的实体

根据不同的情况，订户、HBCA、注册机构、国家法律部门、政府主管部门及其他公共权力部门可以请求吊销最终用户证书。

4.9.3 吊销请求的流程

证书吊销请求的处理采用与原始证书签发相同的过程。

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。其他吊销原因的吊销请求必须在 48 小时内提出。

4.9.5 CA 处理吊销请求的时限

HBCA 或注册机构接到吊销请求后立即处理，24小时生效。

4.9.6 依赖方检查证书吊销的要求

依赖方是否检查证书吊销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，数字证书在此只起身份鉴别的作用，在这种情况下检查证书是否吊销不一定是必须的。

4.9.7 CRL 发布频率

HBCA 每 24 小时更新和公布一次证书吊销列表（CRL）。

HBCA 根据情况，可以自主决定缩短产生和更新 CRL 的时间。

4.9.8 CRL 发布的最大滞后时间

一个证书从它被吊销到它被发布到 CRL 上的滞后时间不超过 24 小时。

4.9.9 在线状态查询的可用性

HBCA 提供 7×24 小时的证书状态查询服务。即在网络允许的情况下，订户能够实时获得证书状态查询服务。

4.9.10 在线状态查询要求

依赖方是否进行在线状态查询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，数字证书在此只起身份鉴别的，在这种情况下在线状态查询不一定是必需的。对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，依赖方在信赖一个证书前必须通过证书状态在线查询检查该证书的状态。

4.9.11 吊销信息的其他发布形式

除了 CRL、OCSP 外，HBCA 的 LDAP 可提供 CRL 的查询。

4.9.12 密钥损害的特别要求

无论是最终订户还是 HBCA、注册机构，发现证书密钥受到安全损害时应立即吊销证书。

4.9.13 证书挂起的情形

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

1、证书订户要求暂停使用该证书一段时间。

2、订户未能履行与HBCA 签订的协议中应尽的义务，但向HBCA 提出申请并获得批准后。

3、除证书订户（或者其授权的委托代理人）外的其它实体，如电子认证服务机构及其授权的服务机构、法院、政府主管部门及其他公共权利部门。向HBCA 提出挂起证书请求并获得批准。

场景证书不涉及证书挂起。

4.9.14 请求证书挂起的实体

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

4.9.15 证书挂起和恢复（解挂）的流程

订户在申请证书挂起和恢复（解挂）时，由HBCA 受理点根据申请变更的证书种类，发放相应的申请表，订户填写完后，受理点根据申请表进行证书挂起或恢复（解挂）注册等制作工作。

订户在申请办理电子认证证书挂起或恢复（解挂）时，有责任在证书申请中提供准确有效的信息，提供相关的证明文件。

4.9.16 挂起的期限限制

申请证书挂起的期限为：在证书有效期剩余的时期内。

4.10 证书状态服务

4.10.1 操作特征

HBCA 通过 CRL、OCSP 提供证书状态查询服务。

4.10.2 服务可用性

HBCA 提供 7×24 小时的证书状态查询服务。即在网络允许的情况下，订户能够实时获得证书状态查询服务。

4.10.3 可选特征

无

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：

1、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；

2、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

4.12.1 密钥生成、备份与恢复的策略与行为

HBCA签发的订户证书中，含有签名用途的密钥对由订户生成或由HBCA提供的密码模块（如智能密码钥匙）生成。为保证订户签名私有密钥的唯一性和安全性，HBCA任何所属机构不对该密钥对进行保管和备份，提醒并要求订户妥善保管。由于签名私有密钥遗失或被窃取所造成的损失由订户自己承担，HBCA 概不负责。而加密用途的密钥对则由密钥管理中心产生、备份和托管。密钥管理中心由密码主管部门直接或委托HBCA管理。

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。

1、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解密，此时订户可申请密钥恢复。订户在 CA 机构或授权的注册机构申请，经审核后，通过 CA 机构向密钥管理中心请求；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。

2、司法取证密钥恢复：司法取证人员在密钥管理中心申请，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。

场景证书的签名密钥由签名设备生成密钥并执行签名后，即时销毁。场景证书没有加密密钥，不提供密钥备份与恢复服务。

协同证书的签名密钥对由国家密码管理部门认可的密码模块生成，不提供签名密钥的备份与恢复服务。加密密钥对由密钥管理中心生成，密钥管理中心负责加密密钥的备份与恢复服务。

4.12.2 会话密钥的封装与恢复的策略与行为

非对称算法组织数字信封的方式来封装会话密钥。数字信封使用信息接受者的公钥对会话密钥加密，接受者用自己的私钥解开并恢复会话密钥。

5. 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

HBCA 认证业务运营场地位于湖北省武汉市武昌区华中小龟山金融文化公园 9 栋，HBCA 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，它可以对个人的进入提供强制性的控制；并且每个个人要进入下一个区域，必须得到相应的授权方可进入。

机房设施的建筑物理安全标准，已通过国家密码管理局的安全性审查。敏感区域采用屏蔽机房建设；使用了一个监控室作为从外部区域进入敏感区域的的常规入口。

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。机房的所有门都足够结实，能防止非法的进入。机房通过设置门禁和监控系统重点保护机房物理安全。

物理访问控制包括如下几个方面：

1、任一道门每次进出都有记录作为审计依据；

2、系统采用身份识别卡和生物识别双重鉴定的控制方法，控制每道门的进入，进入需要两人以上鉴定通过，退出需要一人鉴定通过；

3、与门禁系统配合使用的还有视频监控系统，所有的视频录像资料根据安全审计要求保留一段时间。

4、整套访问控制系统配有断电保护装置，并提供至少 4 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，计算机设备和动力设备分开供电。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。计算机设备专用配电柜和辅助设备配电柜独立设置。

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，在单路电源损坏时，可以维持系统正常运转。

根据机房环境及设计规范要求，HBCA 系统机房使用中央空调,进行温度和湿度的调控，并额外配备湿度控制设备来应对过湿天气。

5.1.4 水患防治

机房在建设初期已采取抬高机房地面与外部地面相对位置、修建挡水坝、屏蔽机房外壳涂刷防水涂料等积极措施，防止水侵蚀和锈侵蚀，充分保障系统安全。

5.1.5 火灾防护

HBCA 物理环境建设时消防报警系统和灭火系统均通过了公安消防部门的消防验收。

在 HBCA 机房内、各物理区域内均设置了烟、温感探测器。

机房区域配置了独立的气体灭火装置。

5.1.6 介质存储

HBCA 对储存产品软件和数据、归档、审计或备份信息的介质保存在安全设施中，这些设施受到适当的物理和逻辑访问控制的保护，只允许授权人员的访问，并防止这些介质受到意外损坏（如水、火灾和电磁）。

5.1.7 废物处理

当 HBCA 存档的敏感数据或密钥已不再需要或存档的期限已满时，应当由相应的数据管理人员将这些数据进行销毁。写在纸张之上的，必须切碎或烧毁。如果保存在

磁盘中，应多次重写覆盖磁盘的存储区域，其他介质以不可恢复原则进行相应的销毁处理。

5.1.8 异地备份

HBCA 对关键系统数据、审计日志数据和其他敏感信息进行日常备份，这些备份信息保存在 HBCA 建筑物以外的安全的地方。

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，都是可信角色，必须由可信人员担任。

可信角色包括：

- 超级管理员
- 系统管理员
- 密钥管理员
- 安全管理员
- 审计管理员
- 证书业务管理员
- 证书业务操作员

5.2.2 每项任务需要的人数

HBCA 确保单人不能接触、备份、恢复、更新、废止 HBCA 存储的根证书对应的私钥。至少三个人才能使用一项对参加操作人员保密的密钥分割和合成技术来进行根密钥的操作。

HBCA 对与运行和操作相关的职能有明确的分工，贯彻互相牵制、互相监督的安全机制。

5.2.3 每个角色的识别与鉴别

所有 HBCA 的在职人员，在进入 HBCA 机房或系统时，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。HBCA 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

HBCA 及 HBCA 的注册机构建立并执行严格的控制流程，根据工作要求和工作安排采取职责分离措施，建立互相牵制、互相监督的安全机制，确保由多名可信人员共同完成敏感操作。HBCA 进行职责分离的角色，包括但不限于下列人员：

1、证书业务受理；

2、系统工程与维护；

3、CA 密钥管理；

4、安全审计。

5.3 人员控制

5.3.1 资格、经历和无过失要求

HBCA 所有的员工必须与 HBCA 签定保密协议。对于充当可信角色或其他重要角色的人员，必须具备一定的资格。HBCA 确立了流程管理和规则，HBCA 员工受到劳动合同、保密协议和规章制度的约束，不得泄露 HBCA 证书服务体系的敏感信息。

HBCA 要求可信人员必须忠诚、可信及工作热情高、无同行业重大错误记录、无违法违纪的记录。HBCA 可信任员工的背景调查由 HBCA 人事部门负责，如有需要，可与有关的政府部门和调查机构合作，完成对 HBCA 可信任员工的背景调查。

5.3.2 背景审查程序

为了确保担任可信角色的人员能够胜任有关工作，HBCA 对雇佣的人员先进行背景调查。在成为 HBCA 的可信人员前，有关人员必须提交相关材料，以证明他们能够胜任预期的工作。

HBCA 依据有关材料进行背景调查，调查人员必须严格遵守保密制度，不得外泄调查情况。

背景调查时如果出现提交材料与事实不符或证明提交材料为捏造时，HBCA 将拒绝可信职位候选人获得有关职位或取消其可信人员的资格。

5.3.3 培训要求

HBCA 对员工进行综合性的培训，培训内容包括：

1、职业行为规范及岗位职责。

2、安全管理要求及公司管理制度。

3、保密制度及相关法律法规。

4、PKI 及应用。

5、HBCA 的产品与服务。

6、其他需要进行的培训。

5.3.4 再培训周期和要求

HBCA 根据业务需要安排。对于充当可信角色或其他重要角色的人员，每年至少接受 CA 机构组织的培训一次。认证策略调整、系统更新时，应对全体人员进行再培训，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，HBCA 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

HBCA 对于未授权行为或其他违反公司安全策略和程序的行为制定有相应的处罚措施，包括警告、罚款直至辞退。

当发现员工滥用权利或越权操作，将立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。对情节严重的，依法追究相应责任。

5.3.7 独立合约人的要求

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

1、人员档案进行备案管理；

2、具有相关业务的工作经验；

3、必须接受 HBCA 组织的岗前培训和继续培训；

4、必须签定《保密协议》。使其能够严格遵守 HBCA 的规范体系。

5.3.8 提供给员工的文档

为使得系统正常运行，HBCA 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

HBCA 须记录与 CA 和 RA 运行系统相关的事件。这些记录应包含事件内容、事件发生的时间和事件相关实体身份。

1、证书订户服务流程中产生的信息数据和资料，如申请表、协议、身份资料等。

2、认证系统日常运作产生的日志记录文件。

3、进出敏感区域的工作记录。

4、可信角色人事变动的相应记录。

5、认证机构、注册机构和审核受理点之间的协议、规范和相关工作记录。

6、其它按规定需要记录的内容。

5.4.2 处理日志的周期

HBCA 每月对日志进行审查，并对审查日志的行为进行备案。

5.4.3 审计日志的保存期限

HBCA 审计日志每月形成新的归档文件进行保存。归档之后保存期限不低于 5 年。

5.4.4 审计日志的保护

HBCA 执行严格的管理，确保只有 HBCA 授权的人员才能对审查日志进行相应操作。日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、修改和删除等操作，另外对日志进行异地备份。

5.4.5 审计日志备份程序

对于认证系统的日志，HBCA 定期进行备份。

5.4.6 审计收集系统

无。

5.4.7 对导致事件实体的通告

针对审计记录中不同性质和类型的事件，HBCA 将记录事件发生的相关方以及其行为和发生的时间位置等信息，并保留采取相应措施的权利。当审计记录报告一个事件时，HBCA 有权决定是否通告引起该事件的个人、组织机构或其他实体。

5.4.8 脆弱性评估

HBCA 每年对系统进行漏洞扫描和渗透测试等脆弱性评估，并根据评估报告采取措施，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

HBCA 归档记录的类型见 CPS § 5.4.1。

5.5.2 归档记录的保存期限

HBCA 所有归档文件的保存期一般规定为五年。

HBCA 订户证书的归档至少保存到证书有效期结束后五年。

CA 证书和密钥的归档在 CA 证书和密钥生命周期之外，额外保留五年。

5.5.3 归档文件的保护

HBCA 对各种电子、磁带、纸资形式的归档文件，都有安全的物理和逻辑保护措施和严格的管理程序，确保归档了的文件不会被损坏，防止非授权的访问、修改、删除或其它的篡改行为。

5.5.4 归档文件的备份程序

所有存档的文件和数据库保存在 HBCA 主机房的存储库，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。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。HBCA 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 记录时间要求

HBCA 对每项日志有时间记录。

5.5.6 归档收集系统

HBCA 的档案收集系统由人工操作和自动操作两部分组成。

5.5.7 获得和检验归档信息的程序

只有可信人员才可以查看和获得归档信息，这些信息被归还时必须得到验证。

5.6 电子认证服务机构密钥更替

当 CA 密钥对的累计寿命超过本《电子认证业务规则》6.3.2 中规定的最大生命期，或因其他特殊原因需要变更 CA 密钥的，HBCA 将启动密钥更新流程，替换原有 CA 密钥对。HBCA 密钥变更按如下方式进行：

1、一个上级 CA 将在其私钥到期时间小于下级 CA 的生命期之前停止签发新的下级 CA 证书（“停止签发日期”）；

2、产生新的密钥对，签发新的上级 CA 证书；

3、在“停止签发日期”之后，对于批准的下级 CA（或订户）的证书请求，将采用新的 CA 密钥签发证书；

4、上级 CA 继续利用原来的 CA 私钥签发 CRL 直到利用原私钥签发的最后的证书过期为止。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

发生故障时，HBCA 将按照相应恢复计划实施恢复。

5.7.2 计算机资源、软件和/或数据的损坏

HBCA 对业务系统及其他重要系统的资源、软件和/或数据进行了备份，并制定了相应的应急处理流程，当出现计算机资源、软件和/或数据的损坏时在最短的时间内恢复被损害的资源、软件和/或数据。

5.7.3 实体私钥损害处理程序

对于实体私钥的损害，HBCA 有如下处理要求和程序：

1、当证书订户发现实体证书私钥损害时，订户必须立即停止使用其私钥，并立即前往 HBCA 或相应的注册机构申请注销其证书。

2、当 HBCA 或注册机构发现证书订户的实体私钥受到损害时，HBCA 或注册机构将立即吊销证书，并通知证书订户，订户必须立即停止使用其私钥。

3、当 HBCA 的 CA 证书出现私钥损害时，HBCA 将立即吊销 CA 证书并及时通过广达的途径通知依赖方，然后生成新的 CA 密钥对、签发新的 CA 证书。

5.7.4 灾难后的业务连续性能力

HBCA 针对证书系统的核心业务系统,证书签发系统和证书接口系统采用双机热备方式；对核心数据库，证书管理系统数据库采用磁盘阵列方式来确保证书系统的高可靠性和可用性。除非物理场地出现了毁灭性的、无法恢复的灾难。

5.8 CA 或 RA 的终止

当 HBCA 及其注册机构需要停止其业务时，将会严格按照《中华人民共和国电子签名法》、《电子认证服务管理办法》中对认证机构中止业务的规定要求进行有关工作。

6. 认证系统技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

6.1.1.1 CA 密钥对的产生

CA 根密钥对由 HBCA 专门的密钥管理员及若干名可信雇员按照密钥管理策略中规定的密钥生成规程产生。CA 根密钥生成、保存的密码模块符合国家密码主管部门的要求，并具有国家密码主管部门的相应资质。

6.1.1.2 最终订户密钥对的产生

订户的签名密钥对应使用密码模块产生由订户负责，订户应确保其密钥产生的可靠性，并负有保护其私钥安全的责任和义务，并承担由此带来的法律责任。

订户的加密密钥对是由国家密码管理局许可的、HBCA 数字证书签发系统通过安全通道连接的密钥管理系统（以下简称 KMC）产生，并通过安全方式传输给订户。KMC 接受湖北省密码管理局的监管。

如果 HBCA 或其注册机构 RA 获知订户私钥交予了未授权人员或不与订户关联的组织，HBCA 将撤销该私钥所对应的公钥证书。

场景证书的密钥对由订户或订户授权的负责该场景业务的系统建设方产生，并负责保护场景证书私钥的安全。

6.1.2 私钥传送给订户

证书订户的加密私钥是在 KMC 产生的，该私钥只保存在 KMC 和订户自行保管的密码模块中。加密机私钥通过安全通道从 KMC 转递到订户的密码模块中，保证了证书订户的密钥安全。

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 RA 传递到 HBCA 数字证书签发系统。

订户的加密证书公钥，由 KMC 通过安全通道传递到 HBCA 数字证书签发系统。

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。

6.1.4 CA 公钥传送给依赖方

对于 HBCA 的根 CA 公钥，可通过如下四种方式传输给依赖方：

1、依赖方可以通过 HBCA 的网站下载 HBCA 根证书；

2、HBCA、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；

3、HBCA、注册机构或其合作伙伴通过电子邮件将 CA 证书传输给依赖方；

4、HBCA、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 HBCA 根证书。

6.1.5 密钥的长度

HBCA 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 HBCA 电子认证系统支持签发 SM2-256、RSA-2048、RSA-1024 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管理部门许可的密码设备或密码模块生成。对生成的公钥参

数的质量检查标准，内置的协议、算法等均符合国家密码管理部门要求。

6.1.7 密钥使用目的

在 HBCA 证书服务体系中的密钥用法和证书类型紧密相关。

订户证书依据应用场景配置密钥用法及增强密钥用法，即，用于数字签名（包括身份验证）的证书将设置数字签名及/或不可否认的密钥用法，用于密钥或数据加密的证书将设置密钥加密及/或数据加密的密钥用法，用于密钥协商的证书将设置密钥协商的密钥用法。每种订户证书中至少包含两种密钥用法或增强密钥用法。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块的标准和控制

HBCA 使用国家密码管理局许可的产品，密码模块的标准符合国家规定的要求。

1、接口安全:不执行规定命令以外的任何命令和操作;

2、协议安全:所有命令的任意组合，不能得到私钥的明文;

3、密钥安全:密钥的生成和使用必须在硬件密码设备中完成;

4、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 私钥多人控制

根 CA 系统的私钥存放在符合安全要求的加密机中，该加密机的管理密钥被分割保存在多个智能密码钥匙或 IC 卡中，这些智能密码钥匙或 IC 卡分别由多名 HBCA 的可信雇员持有（称为密钥分管者），保存在 HBCA 内部保险盒中。当要操作使用 CA 私钥时（如生成、更新、销毁、备份和恢复等），需要按照加密机的安全机制由多名密钥管理者持保存有分割密钥的智能密码钥匙或 IC 卡通过加密机验证后才能由授权人员进行相应操作。

订户的私钥由订户通过密码设备或密码模块的密码、口令来控制。

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托管，订户的签名证书对应的私钥由自己保管或控制，密钥管理中心不负责托管签名私钥。

密钥管理中心严格保证订户密钥对的安全，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

HBCA 对 CA 私钥通过专门的备份 IC 卡进行备份，备份操作将按照 CPS § 6.2.10 私钥多人控制的机制进行。

对于最终订户证书，HBCA 不备份订户的签名密钥，HBCA 建议订户对签名密钥进行备份，并对备份的签名密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。KMC 备份托管加密私钥，确保加密私钥的安全。

6.2.5 私钥归档

当 HBCA 的 CA 密钥对到期后，这些 CA 密钥对将归档保存至少 5 年。并且 HBCA 的密钥管理策略和流程阻止归档的 CA 密钥对返回到生产系统中。对归档私钥到了归档保存期，HBCA 将按 CPS § 6.2.10 销毁。

KMC 提供过期的托管加密私钥的归档服务。

6.2.6 私钥导入、导出密码模块

HBCA 的 CA 密钥对在硬件密码模块上生成，保存和使用。HBCA 制定了相关的密钥管理策略来有效防止 CA 私钥的丢失、被窃、修改、泄露、非授权的使用。为了常规恢复和灾难恢复，HBCA 对 CA 密钥进行备份。当 CA 密钥对从一个硬件密码模块复制到另一个硬件密码模块上时，备份的密钥对以加密的形式在模块之间传送。

6.2.7 私钥在密码模块的存储

HBCA 采用国家密码管理部门认可的密码设备，这些设备内置的协议、算法等均

符合国家密码行业的标准要求。

订户私钥在密码设备或密码模块中加密保存。

6.2.8 激活私钥的方法

6.2.8.1 CA 私钥

CA 私钥存放在硬件密码设备中，具有激活私钥权限的管理员使用含有自己的身份的智能 IC 卡登录，启动密钥管理程序，进行激活私钥的操作，需要半数以上的管理员同时在场。

6.2.8.2 订户私钥

当订户私钥存放在软件密码模块中时，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。

当订户私钥存放在诸如 USB Key 和智能卡等硬件密码模块中，这时私钥可以通过 PIN 码（口令）或指纹鉴别等安全机制保护。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）或指纹鉴别保护，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）或指纹信息，私钥才被激活可以使用。

订户应该采用合理的措施保护密码模块以防止在没有得到订户授权的情况下被其他人员使用。

6.2.9 解除私钥激活状态的方法

对于订户私钥，当密码模块被卸载、移除、系统注销、关闭或断电时，私钥被解除激活状态。

对于 HBCA 私钥，当存放私钥的硬件密码模块断电，私钥进入非激活状态。

6.2.10 销毁私钥的方法

HBCA 的 CA 密钥需要销毁时，应按照§6.2.2 的私钥多人控制方式由多名密钥分管者通过加密机验证后由具有销毁密钥权限的管理员进入加密机管理程序，进行销毁密钥的操作。

当订户私钥过期或发现不安全时，应按照存储私钥的密码模块的说明完成私钥销毁。订户在销毁私钥前，须自行确认是否还有信息需要加密私钥进行解密。由于订户销毁私钥导致的原有信息无法解密的后果，需由订户自行承担，HBCA 不承担任何责任。

6.2.11 密码模块的评估

HBCA 使用通过检测认证的服务器密码机，符合国家有关标准。密码机采用以分组密码体制为核心的高强度密码算法和非对称密码体制，密钥采取分层结构，逐层提供保护。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

对于生命周期外的 CA 和最终订户证书，HBCA 将进行定期归档，归档的证书存放在归档数据库中。

6.3.2 证书操作期和密钥对使用期限

CA 证书有效期不超过 30 年。CA 密钥对使用期限和 CA 证书有效期保持一致。所有订户签名密钥对的使用期限和订户证书的有效期保持一致，加密密钥对在保证安全的前提下可根据订户要求或证书应用的需要适当延长使用期限。特殊情况下，对于签名类证书为了验证在证书有效期内签名的信息，与之对应的公钥可以在证书的有效期限以外使用，直到私钥受到损害或密钥对存在被破解的风险，如加密算法被破解。

6.4 激活数据

6.4.1 激活数据的产生与安装

CA 私钥的激活数据由服务器密码机内部产生，并分割保存在多个 IC 卡中，需通过服务器密码机内置的读卡设备和软件读取。

订户证书的密钥存储在密码设备（如：智能密码钥匙）或密码模块中，激活数据为 PIN 码（口令），由订户在初始化密码设备或密码模块时自行设置。对于非一次性使用的激活数据，建议用户自行进行修改。HBCA 要求订户设置的 PIN 码（口令）长度不少于 6 位字符（英文字母或数字）。

6.4.2 激活数据的保护

保存有 CA 私钥的激活数据的多个 IC 卡分别依据 HBCA 职责分割的要求由多名不同的可信管理人员掌管。

订户的激活数据是私钥保护密码，如果证书订户使用口令或 PIN 码保护私钥，订户应妥善保管好其口令或 PIN 码，防止泄露或被窃取。如果证书订户使用生物特征保护私钥，订户也应注意防止其生物特征被人非法获取。

6.4.3 激活数据的销毁

HBCA 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，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 § 6.2.5 的规定处理。

订户私钥的激活数据在不需要时由订户自行销毁，订户应确保他人无法通过残余信息、存储介质直接或间接地恢复激活数据。

6.4.4 激活数据的其他方面

考虑到安全因素，对于订户激活数据的生命周期，规定如下：

用于保存私钥的密码模块的 PIN 码（口令），建议订户根据业务应用的需要随时予以变更，使用期限超过 3 个月后需要进行修改。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

HBCA 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，其他人员不能操作和控制 HBCA 系统；其他普通用户无系统账号和密码。HBCA 系统部署防火墙、入侵防御系统以及防病毒系统，确保系统网络安全。本系统采用增加冗余资源的方法，提高系统可用性。

6.5.2 计算机安全评估

HBCA 电子认证服务系统已经通过国家密码管理局的安全性审查，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

6.6.1 系统开发控制

HBCA 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。

6.6.2 安全管理控制

HBCA 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。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。

6.6.3 生命期的安全控制

HBCA 和相关产品开发商以及标准机构共同合作，整个系统从设计到实现，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管理部门鉴定，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，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。HBCA 对系统的任何修改和升级会记录在案并予以控制。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。

6.7 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。HBCA 采取防火墙、病毒防治、入侵防御、漏洞扫描、数据备份、灾难恢复等安全防护措施。

7. 证书、证书吊销列表和在线证书状态协议

7.1 证书

HBCA 签发的证书均符合 X.509 V3 证书格式。遵循 RFC5280 标准。

7.1.1 版本号

X.509 V3 证书。

7.1.2 证书扩展项及其关键性

证书扩展项是一个或多个证书扩展的序列。针对某种证书类型或者特定用户，HBCA 签发的证书除使用 IETF RFC 5280 中定义的证书扩展项外，还支持私有（非关键）扩展项，不能识别私有（非关键）扩展项的应用、依赖方可以忽略该扩展项。

7.1.3 算法对象标识符

HBCA 签发的证书符合 RFC5280 标准，采用 sha1RSA、sha256RSA、sm2withSM3 签名算法签名。

sm2withSM3 签名算法的 OID 为：1.2.156.10197.1.501

sha256RSA 签名算法的 OID 为：1.2.840.113549.1.1.11

sha1RSA 签名算法的 OID 为：1.2.840.113549.1.1.5

7.1.4 名称形式

HBCA 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 和 OU，其格式如下：

1、C（Country）应为 CN，表示中国；

2、O（Organization）代表证书持有者所在的组织机构；

3、OU（Organization Unit）代表证书持有者所在的部门；

4、CN（Common Name）中的内容分为 4 种：

a）个人证书中应为证书主体的姓名；
b）机构证书中应为证书主体单位的标准全称或简称；
c）设备证书应为证书主体设备的域名或者IP地址或者设备编码；
d）场景证书中代表电子签名人的实体信息。

5、Email 代表电子邮件地址。

7.2 证书吊销列表

7.2.1 版本号

HBCA 签发的证书吊销列表遵循 RFC5280 标准。采用 X.509 V2 格式。

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 编号（CRL Number）

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

使用 OCSP 版本 1（OCSP v1）。

7.3.2 OCSP 扩展项

不使用 OCSP 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

评估审计是为了检查、确认HBCA是否按照《电子认证业务规则》及其业务规范、管理制度和安全策略开展业务，发现存在的可能风险，以达到规避经营风险、提高服务质量、保障客户权益的目的。

评估审计分内部审计和外部审计。

内部审计是由HBCA组织内部审计人员进行的至少一年一次的定期审计。HBCA可根据业务发展情况，自行决定内部审计范围（包括但不限于对RA的审计）。审计的结果可供HBCA 改进、完善业务，内部审计结果不需要公开。

外部审计是由法律规定的主管部门、主管部门委托的第三方机构或 HBCA 委托的第三方机构对自身的电子认证服务业务进行审计与评估。审计内容、评估标准及审计评估结果是否公开由主管部门确定。

8.2 评估者的资质

内部审计人员的选择一般包括：

1、HBCA 的安全策略委员会成员；

2、HBCA 的业务负责人；

3、认证系统及信息系统负责人；

4、人事负责人；

5、其他需要的人员。

外部审计的审计人员的资质由第三方确定。

8.3 评估者与被评估者之间的关系

评估者应是与被评估者之间无任何业务、财务往来或其他足以影响评估客观性的利害关系的机构或组织。

8.4 评估内容

审计所涵盖内容应该包括：

1、CA 物理环境和控制；

2、密钥管理操作；

3、基础 CA 控制；

4、证书生命周期管理；

5、CA 业务规则。

8.5 对问题与不足采取的措施

对审计中发现的问题，HBCA 将根据审计报告的内容准备一份解决方案，明确对此采取的行动。HBCA 将根据国际惯例和相关法律、法规解决问题。

8.6 评估结果的传达与发布

审计结果将传达给 HBCA 安全策略委员会。

除非法律明确要求，HBCA 一般不公开审计结果。

对于关联方，HBCA 将依据签署的协议来公开审计结果。

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

HBCA 数字证书的收费标准参照市场和湖北省物价主管部门批准的收费标准执行。根据证书的实际应用需要，HBCA 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，HBCA 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，HBCA 不收取信息访问费用。

对于在线证书状态查询（OCSP），由 HBCA 与依赖方或订户在协议中约定。

9.1.4 其他服务费用

HBCA 可根据请求者的要求，订制各类服务，具体服务费用由 HBCA 在与订制者签订的协议中约定。

9.1.5 退款策略

在实施证书操作和签发证书的过程中，HBCA 遵守并保持严格的操作程序和策略。一旦订户接受数字证书，HBCA 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，HBCA 将不退还剩余时间的服务费用。

9.2财务责任

9.2.1 保险范围

HBCA根据业务发展情况和国内保险公司的业务开展情况决定其投保策略。

9.2.2 对最终实体的保险或担保

HBCA 保证具有维持运作和履行其责任的财务能力。

HBCA 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》的规定进行赔偿。具体的情况及赔付额度，参见本《电子认证业务规则》9.9。

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：

1、在双方披露时标明为保密(或有类似标记)的；

2、在保密情况下由双方披露的或知悉的；

3、双方根据合理的商业判断应理解为保密数据和信息的；

4、以其他书面或有形形式确认为保密信息的；

对于 HBCA 来说，保密信息包括但不限于以下方面：

1、最终用户的私人签名密钥都是保密的；

2、保存在审计记录中的信息；

3、年度审计结果也同样视为保密；

除非有法律要求，由 HBCA 掌握的，除作为证书、CRL、认证策略被清楚发布之外的个人和公司的信息需要保密。

HBCA 不保存任何证书应用系统的交易信息。

除非法律明文规定，HBCA 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、申请操作指南等资料中公布的信息是公开的。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。

HBCA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。

以上信息虽然不属于保密信息，但任何个人或组织不得转载或用于任何商业用途，HBCA 保留追究责任的权利。

9.3.3 保护保密信息的责任

HBCA 有各种严格的管理制度、流程和技术手段用以保护客户机密信息。HBCA 的每个员工都要与公司签订保密协议。

9.4个人隐私保密

9.4.1 隐私保密方案

依据相关法律、法规，HBCA在受理订户申请证书及相关电子签名业务时，需由证书申请者或经办人提供相关信息。其中个人信息可能包括：姓名、联系方式、身份证号码、住址和身份证（原件及/或任何形式的复本）等个人隐私信息。

本《电子认证业务规则》有关用户个人信息保护条款的完整内容见HBCA官方网站（https://www.hbca.org.cn/）公布的《个人信息保护政策》。

9.4.2 作为隐私处理的信息

证书申请者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

证书申请者提供的用来构成数字证书内容的资料不认为是隐私信息。

9.4.4 保护隐私的责任

HBCA 和授权的注册机构、受理点在没有获得订户授权的情况下，不得将订户隐私

信息透露给第三方。但当HBCA在法律、行政法规、规章的规定下，或在行政机关、司法机关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，HBCA可以按照法律、法规、规章以及司法机关的要求，向有关部门提供相关的保密信息。这种信息披露不视为违反了保护隐私的义务，HBCA无须承担任何责任。

9.4.5 使用隐私信息的告知与同意

HBCA 只在其业务范围内使用 9.4.2 所列的隐私信息，包括订户身份识别、管理、和服务的目的。对于业务范围内的隐私信息使用，HBCA 没有告知订户的义务，也无需得到订户的同意。

HBCA 不会在使用证书服务及应用无关的系统或场合使用订户个人信息。出现下列情形之一的，HBCA 将依法提供用户个人相关信息：

1、基于国家法律、行政法规、规章的规定而提供的；

2、基于行政机关、司法机关的要求下而提供的；

3、经过订户本人书面授权或同意提供的。

除上述情形外，HBCA 不会向任何第三方提供订户的个人信息，不会将订户个人信息用于其他用途。

9.4.6 依法律或行政程序的信息披露

当 HBCA 在国家法律、行政法规、规章的规定下，或在司法机关的要求下必须提供证书申请者的特定资料或隐私信息时，HBCA 按照法律、法规或规章的规定或司法机关的要求，向有关部门公布相关信息，HBCA 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

除非额外声明，HBCA享有并保留对证书以及所提供的全部软件的一切知识产权，包括但不限于所有权、名称权、著作权、专利权和利益分享权等。HBCA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。

HBCA制订并发布的CPS、CP、技术支持手册、发布的证书和CRL等的所有权和知识产权均归属于HBCA。

9.6 陈述与担保

除非 HBCA 作出特别约定，若本认证业务规则的规定与 HBCA 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 HBCA 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。

9.6.1 电子认证服务机构的陈述与担保

HBCA 在提供电子认证服务活动过程中的承诺如下：

1、HBCA 遵守《中华人民共和国电子签名法》及相关法律的规定，接受工业和信息化部的领导，对签发的数字证书承担相应的责任与义务。

2、HBCA 保证使用的系统及密码符合国家政策与标准，保证自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。

3、HBCA 签发给订户的证书符合本《电子认证业务规则》的所有实质性要求。

4、HBCA 将向证书订户通报任何已知的、将在本质上影响订户的证书的有效性和可靠性事件，通报的有效形式包括但不限于邮件通知、官网公告。

5、HBCA 将及时吊销证书，并发布到 CRL 上供订户查询。

6、证书公开发布后，HBCA 向证书依赖方承诺，除了未经鉴别的订户信息外，数字证书中载明的订户信息都是准确的。

9.6.2 注册机构的陈述与担保

HBCA 授权的注册机构、受理点在参与电子认证服务过程中的承诺如下：

1、提供给证书订户的注册过程完全符合 HBCA《电子认证业务规则》的所有实质性要求。

2、在 HBCA 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者的信息不一致。

3、注册机构将按照本《电子认证业务规则》的规定，及时响应并向 HBCA 提交订户证书申请、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 HBCA 签发的证书，就被视为向 HBCA、注册机构及证书依赖方的有关当事人作出以下承诺：

1、订户已阅读并理解本《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。

2、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，可供 HBCA 或注册机构检查和核实。

3、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。

4、私钥为订户本身访问和使用，订户对使用私钥的行为负责。

5、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 HBCA 和注册机构，申请采取吊销等处理措施。

6、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 HBCA 吊销其证书。

9.6.4 依赖方的陈述与担保

证书依赖方必须熟悉本《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理解本《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 HBCA 的责任。

1、如果证书申请者故意或过失提供了不准确、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 HBCA 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者全部承担。HBCA 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。

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

3、在法律许可的范围内，根据有关法律法规的要求，如实提供电子交易和网络交易中产生的电子签名的验证信息，HBCA 不承担由此引起的任何法律责任。

4、HBCA 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。

5、由于客观原因和其他不可抗力因素导致 HBCA 暂停、终止部分或全部数字证书服务，HBCA 不承担赔偿或补偿责任。

这些客观原因包括但不限于：（1）不可抗力；（2）关联单位如电力、电信、通讯部门中止或停止服务；（3）黑客攻击；（4）HBCA 已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则的。关于不可抗力的描述详见 9.16.5。

6、HBCA 与授权的外部注册机构或依赖方签署合同，合同条款中明确注册机构或依赖方承担订户身份核实责任。对于明显由于外部注册机构或依赖方的越权行为或其他过错行为所引发的违反约定义务而对订户造成的损失，由授权的外部注册机构或依赖方承担。

7、订户因证书丢失、私钥泄漏等原因需办理挂失、注销手续的。自订户申请办理挂失或注销时起之后的 24 小时内造成的损失，HBCA 不承担相关责任。

8、HBCA 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经 HBCA 允许的用途，HBCA 不承担任何法律责任 。

9.8 有限责任

HBCA 根据与订户的协议承担相应的有限责任。

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

9.9 赔偿

HBCA 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。HB 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。

HBCA 对于 HBCA 的数字证书订户有限赔偿责任的赔偿金额上限为该订户实缴该数字证书开户费或年服务费的十倍。

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。HBCA 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 HBCA 和注册机构名誉或经济损失，订户和依赖方应承担赔偿 HBCA 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。

1、未向 HBCA 提供真实、完整和准确的信息，而导致 HB CA 或有关各方损失。

2、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。

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

4、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。

5、证书的非法使用，即违反 HB CA 对证书使用的规定，造成了 HB CA 或有关

各方的利益受到损失。

9.10 有效期限与终止

9.10.1 有效期限

《电子认证业务规则》在 HBCA 官方网站（https://www.hbca.org.cn）公布之日起生效, 除非 HBCA 特别声明《电子认证业务规则》提前终止。

《电子认证业务规则》中将详细注明版本号及发布日期，最新版本请访问 HBCA 官方网站，对具体订户和依赖方不做另行通知。

9.10.2 终止

当新版本的《电子认证业务规则》正式公布生效时，旧版本的《电子认证业务规则》自动终止。

9.10.3 效力的终止与保留

《电子认证业务规则》中涉及的隐私保护、知识产权以及涉及赔偿的有限责任条款，在终止后继续有效。

9.11 对参与者的个别通告与沟通

HBCA 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其他违反订户协议的行为时，可通过适当方式（如电话、电邮、信函、传真等）个别通知订户、依赖方。

9.12 修订

9.12.1 修订程序

当本《电子认证业务规则》不适用时，由 HBCA 安全策略委员会组织编写小组进行修订。修订完成后，HBCA 安全策略委员会进行审批，审批通过后将在官方网站

(https://www.hbca.org.cn）上发布新版的《电子认证业务规则》。

9.12.2 通知机制和期限

本《电子认证业务规则》在 HBCA 的网站上发布。版本更新时，最新版本的电子认证业务规则会在 HBCA 的网站公布，对具体订户和依赖方不再另行通知。

9.12.3 必须修改业务规则的情形

当管辖法律、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

HBCA、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HBCA，根据本《电子认证业务规则》中的规定，明确责任方;

2、由HBCA相关部门负责与当事人协调；

3、若协调不成，当事人因与HBCA或授权机构在电子认证活动中产生的任何争端及或对本《电子认证业务规则》所产生的任何争议，均应提请武汉仲裁委员会按照其仲裁规则在武汉进行仲裁。仲裁裁决是终局的，对双方均有约束力。

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用中华人民共和国的相关法律和法规。

9.16 一般条款

9.16.1 完整协议

本《电子认证业务规则》 将替代先前的、与主题相关的书面或口头解释。

9.16.2 转让

HBCA、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

当司法机关或仲裁机构判定本《电子认证业务规则》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《电子认证业务规则》无效。

9.16.4 强制执行

免除一方对《电子认证业务规则》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《电子认证业务规则》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，HBCA 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

HBCA 对本《电子认证业务规则》拥有最终解释权。