湖北省数字证书认证管理中心

电子认证业务规则

版本 **2.0**

湖北省数字证书认证管理中心有限公司

2007 年 **2** 月

目 录

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）缩写为 HBCA ，简称为湖北 CA 。HBCA 是经国家相关部门批准成立的专业化的第三方认证机构。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 IETF RFC 3647（Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,公钥基础设施证书策略和证书运行框架）、《中华人民共和国电子签名法》、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》以及中华人民共和国信息产业部电子认证服务管理办公室编写的《电子认证业务规则规范（试行）》。本 CPS 详细阐述了 HBCA 在实际工作和运行中所遵行的各项规范。本 CPS 作为实际应用和操作的文件依据，适用于所有与 HBCA 有关的终端实体。作为公告，向社会公布 HBCA 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。HBCA 认证体系内的实体以及 HBCA 数字证书持有者，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。

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电子认证业务规则》。

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，也为证书用户提供电子签名认证服务。

1.3.2 注册机构（RA）

注册机构是为最终证书申请者建立注册过程的实体，对证书申请者进行身份标识和鉴别，发起或传递证书吊销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。注册机构作为电子认证服务机构授权委托的下属机构，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。每个注册机构可以按照行业或行政地域分成多个受理点，可以直接对最终用户提供服务。注册机构有责任妥善保存用户的数据，不允许将用户的数据透露给与证书申请无关的任何单位或个人，不允许用作其他商业利益方面的用途。

1.3.3 受理点

受理点负责审核受理证书申请实体的信息，包括申请实体的名称、可以表明身份的号码和联系方法（通信地址、电子邮件、电话）等。受理点根据这些信息为申请实体提供证书，或根据申请实体的要求，提供申请实体自行申请的技术支持。

1.3.4 订户

订户，即证书持有人，是指从 HBCA 申请并接收电子签名认证证书的用户实体。在电子签名应用中，订户即为电子签名人。

1.3.5 依赖方

依赖方即指依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。

依赖方可以是、也可以不是一个订户。

1.3.6 其他参与者

其他参与者指为 HBCA 证书服务体系提供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 电子签名认证证书的应用范围包括电子商务、电子政务、其他社会信息化应用，为建设互联网络的信任环境开展基础性服务。具体请参阅 http://www.hbca.org.cn。

1.4.2 限制的证书应用

HBCA 证书禁止在任何违反国家法律、法规或破坏国家安全的情形下使用，否则由此造成的法律后果由用户自己承担。

1.5 策略管理

1.5.1 策略文档管理机构

本 CPS 的管理机构是 HBCA 运营安全管理小组，由 HBCA 运营安全管理小组负责本 CPS 的制定、发布、更新等事宜。

本 CPS 由湖北省数字证书认证管理中心有限公司拥有完全版权。

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 指定专人负责。

联 系 人：安全管理员

电　　话：027－87823765

传　　真：027－87822397

地　　址：湖北省武汉市水果湖东一路十九号

邮政编码：430071

网站地址：http://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。

1.5.4 CPS 批准程序

HBCA 电子认证业务规则做出任何变动之前，HBCA 运营安全管理小组将对提供的变动建议进行研究，做出变更决定。在征询 HBCA 法律顾问有关法律方面的意见后，形成决议。HBCA 将在决议形成后，在 HBCA 网站公布变更后的 HBCA 电子认证业务规则正式文档，并于公布之日起三十日内报信息产业部备案。

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，是指帮助证书申请者申请证书，批准或拒绝证书申请，吊销证书或更新证书。

电子认证业务规则（CPS）：Certification Practice Statement，电子认证服务机构批准或拒绝证书申请、签发、管理和吊销证书时所遵循规则的详细描述和说明。

证书吊销列表（CRL）：Certificate revocation list，一个定期(或根据要求)发行的、并由发证机关数字签名的信息列表，用来识别在有效期内提前被吊销的证书。

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以及公开密钥的电子文档。

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）：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（电子签名验证数据）：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 HBCA 在公网上发布，用于验证电子签名信息的有效性。

电子签名验证数据：是指用于验证电子签名的数据，包括代码、口令、算法或者公钥。如果电子签名制作数据表现为私钥，则电子签名验证数据就是公钥。

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，订户可以通过访问 HBCA 的目录服务器获取证书的信息和证书吊销列表（CRL）。同时 HBCA 提供在线证书状态查询服务。

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业务的申请者均具备约束力。对具体个人不另行通知。

证书一经签发，HBCA 通过目录服务器自动将该证书公布。

证书一经吊销，HBCA 将立即签发 CRL，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、CPS、CRL 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授权人员才能修改。

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）来唯一标识证书使用者的身份信息。

HBCA 证书符合 X509.3 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。

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	.订户组织机构部门或不用

构部门）	
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： .个人姓名（与身份证上标明的一致） .组织机构名（与营业执照或机构代码证等有效证件上标明的一致） .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，其中的例外是签发双证书时（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，将产生的密钥对放置到智能卡上），那么这个要求不适用。

3.2.2 组织机构身份的鉴别

在组织机构申请者身份的鉴别流程中，HBCA 将按照每种证书的要求进行不同的验证。证书申请表上有申请者本身或被充分授权的证书申请者代表的签字。HBCA 或其注册机构、受理点等电子认证服务机构必须检查申请者所递交的文件，申请者需向HBCA 提供单位或服务器确实存在的有效证明，包括但不限于工商营业执照、企事业单位组织机构代码证等；申请者有义务保证申请材料的真实有效，并遵守责任书、承担与此相关的法律责任。HBCA 和其授权的电子认证服务机构在规定期限内保存组织机构的全部申请材料，这个规定期限由法律、政策、主管部门的要求或者HBCA 自行决定。

3.2.3 个人身份的鉴别

在个人申请者身份的鉴别流程中，HBCA 可以按照每种证书相应的要求进行不同验证。证书申请表上有申请者本身或被充分授权的证书申请者代表的签字。HBCA 或其注册机构、受理点等电子认证服务机构必须检查申请者所递交的文件，申请者需向HBCA 提供申请实体确实存在的有效证明，包括但不限于居民身份证、户口簿、护照、军官证、外国人永久居留证等；申请者有义务保证申请材料的真实有效，并遵守责任书，承担与此相关的法律责任。HBCA 和其授权的电子认证服务机构在规定期限内保存组织机构的全部申请材料，这个规定期限由法律、政策、主管部门的要求或者HBCA 自行决定。

3.2.4 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。

3.2.5 授权确认

为确保办理人具有特定的许可，代表组织获取数字证书，需要出具组织授权其为该组织办理 HBCA 数字证书事宜的授权文件。

组织在 HBCA 的数字证书申请表上加盖单位公章后，则证明本组织对办理人的授权确认。

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。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。为了风险管理和安全考虑，重新申请签发证书时，订户将不被允许使用旧的密钥对，除非订户愿意书面表示自己承担由此产生的一切责任和后果。

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 CPS 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

证书申请实体包括个人和组织机构(包括行政机关、事业单位、企业单位、社会团体和人民团体等)。

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。HBCA 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》的要求准备证书申请材料，并确保申请材料真实准确。

注册机构负责接收证书申请人的请求材料，当面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。

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 CPS 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§3.2.2 组织机构身份的鉴别和§3.2.3 个人身份的鉴别。

4.2.2 证书申请批准和拒绝

在 HBCA 完成对证书申请的鉴证，有关鉴证获得通过并且证书申请者履行了其他应尽的责任（如付款）后，HBCA 或注册机构批准申请。如果鉴证未获通过或证书申请者拒绝履行了其他应尽的责任（如付款），HBCA 或注册机构将会拒绝申请。

4.2.3 处理证书申请的时间

HBCA 及注册机构将在合理时间内完成证书请求处理。在申请者提交资料齐全且符合要求的情况下，处理证书申请的时间不超过 5 个工作日。

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：

a) 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提交给订户，来通知订户证书信息已经正确生成；

b) 邮政信函通知订户；

c) 其他 HBCA 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

HBCA 订户接受证书的方式可以有如下几种：

（1）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。在这种情况下由注册机构替证书订户产生证书请求、证书密钥对、下载证书。

（2）订户通过电子邮件或其他 HBCA 认为合理的方式获取证书的的指示，访问专门的证书下载服务站点将证书下载到本地存放介质，如本地计算机硬盘、USB Key、智能卡。

对于第一种方式，当订户接受了载有证书的介质即表明订户接受了证书。对于第二种方式，系统记录订户下载了证书即表明订户接受了证书

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。

4.4.3 CA 在颁发证书时对其他实体的通告

对于其签发的证书，HBCA 及注册机构不通知其他实体。

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 策略保障的。

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。订户接受到数字证书，应妥善保存其证书对应的私钥。

订户只能在指定的应用范围内使用私钥和证书，订户只有在接受了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。

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。依赖方应将加密证书连同加密信息一起发送给接受方。

4.6 证书更新

4.6.1 证书更新的情形

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。证书订户必须在证书有效期到期前一个月内或已到期后一个月以内，到 HBCA 或 HBCA 授权的发证机构申请更新证书。

出于安全考虑，HBCA 和其授权的证书服务机构默认的方式是证书更新的同时，更新证书的密钥。证书订户也可以选择保留原有密钥，HBCA 一般不建议进行这样的证书更新，但是如果订户提出，HBCA 在考虑到安全和自身利益保障的前提下，可以为订户提供此种服务。

4.6.2 请求证书更新的实体

证书订户、证书订户的授权代表（组织机构证书）或证书对应实体的拥有者（比如服务器证书的拥有者）。

4.6.3 证书更新请求的处理

HBCA 对证书更新请求的处理流程与证书初始注册的流程基本相同。

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。

4.6.8 证书更新的注意事项

请订户在进行证书更新之前将加密邮件等加密过的文件进行解密，同时备份（例如将邮件内容复制以明文方式存储或将邮件附件保存），然后将证书删除。以上操作完成后才能进行证书的更新申请。如订户未解密文件而进行证书更新，由此造成的可能损失，HBCA 概不负责。

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) 因私钥泄漏而吊销证书；
3) 其他。

注：证书吊销后不允许证书密钥更新。

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

证书变更指改变证书中除订户公钥之外的信息而签发新证书的情形。

4.8.1 证书变更的情形

在证书有效期内，当证书信息发生变化，订户或者其它参与者可以选择证书变更，申请签发新的证书。

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

出现以下任何一种情况，最终订户证书必须吊销：

（1）HBCA、注册机构或最终订户有理由相信或强烈的怀疑一个订户的私钥安全已经受到损害。

（2）HBCA 或注册机构有理由相信订户违背了订户协议下的义务、陈述或担保。

（3）HBCA 或注册机构和订户达成的订户协议已经终止。

（4）HBCA 或注册机构有理由相信证书签发时没有依据 CPS 规定的有关程序，证书

签发给了非证书主题的人员或没有鉴证该人员在证书主题中的命名就签发了证书。

（5）HBCA 或注册机构有理由相信证书申请中的信息有违背事实的错误。

（6）HBCA 或注册机构确定证书签发的一个必要前提条件没有满足。

（7）订户的组织机构名改变了。

（8）除了未经鉴证的订户信息外，包含在证书中的信息不正确或已经改变。(包含在证书中的、经过鉴证的信息改变或不正确)

（9）订户请求吊销证书。

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，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 7X24 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。

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，订户填写完后依据申请表按时缴纳相应的费用；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，并按时缴纳相应费用。

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、LDAP 提供证书状态查询服务。

4.10.2 服务可用性

HBCA 提供 7X24 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：

a) 证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，订户可以终止订购；

b) 在证书有效期内，证书被吊销后，即订购结束。

4.12 密钥托管与恢复

湖北省密钥管理中心依国家管理规定，提供加密证书密钥的集中管理和恢复。

4.12.1 密钥托管与恢复的策略与行为

订户加密证书密钥托管与恢复遵循湖北省密钥管理中心内部流程。

注意：为保证订户签名私有密钥的唯一性和安全性，HBCA 不保管签名私有密钥。因此，提醒并要求订户妥善保管。由于签名私有密钥遗失所造成的损失由订户自己承担，HBCA 概不负责。

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武汉市武昌区水果湖东一路十九号省信息中心大楼三楼，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；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。

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）进出每一道门都有记录作为审计依据；

（2）系统采用身份识别卡或生物识别鉴定的控制方法，控制每道门的进出；

（3）与门禁系统配合使用的还有录像监控系统，所有的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。

5.1.4 水患防治

机房在建设初期已采取相应措施，防止水侵蚀，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、导出、恢复、更新、废止 HBCA 存储的根证书对应的私钥。至少三个人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任何钥匙恢复的操作。

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，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

各区管理员有明确的具体角色，以区分任务和责任，如：超级管理员、密钥管理员、以及 HBCA 认可需要职责分割的管理员等。

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。

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。

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：

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 HBCA 组织的岗前培训和继续培训；

d) 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

不公开。

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。

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。归档之后保存期限一般为 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

当审计记录报告一个事件时，HBCA 会立即通知引起该事件的个人、组织机构。

5.4.8 脆弱性评估

HBCA 将定期进行脆弱性评估，并根据评估报告采取措施。

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

内部流程规定。

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 中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

内部流程规定。

5.6 电子认证服务机构密钥更替

HBCA 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。

（1） 使用旧的私有密钥对新的公钥及信息签名生成证书；

（2） 使用新的私有密钥对旧的公钥及信息签名生成证书；

（3）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。

5.7 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 或相应的注册机构吊销其证书，或者立即通过电话、电子邮件等方式通知 HBCA 或注册机构吊销其证书。

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 拥有一套较为完善的系统恢复办法，除非物理场地出现了毁灭性的、无法恢复的灾难，HBCA 能够在出现灾难后最短的时间内恢复其业务能力。

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：

对于HBCA 根密钥对，HBCA 专门的密钥管理员及若干名可信雇员将按HBCA 的密钥管理策略中规定的密钥生成规程进行产生。HBCA 密钥生成规程规定了 CA 密钥产生的流程控制及参加人员。HBCA 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，并通过国家密码主管部门的安全性审查。

6.1.1.2 最终订户密钥对的产生：

订户的签名密钥可以使用浏览器自带的密码模块生成密钥对，也可以使用硬件密码模块（如 USB Key，智能卡）产生密钥对；对于服务器证书，订户利用 Web 服务程序软件提供的密钥生成功能生成密钥对或采用专门的硬件加速模块产生密钥对。

订户的加密密钥对是由国家密码管理局许可的、HBCA 数字证书签发系统支持的

加密机设备生成的，由湖北省国家密码管理局所辖的密钥管理中心管理（以下简称KMC）。

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 和订户介质。

在加密私钥从 KMC 到订户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。HBCA 无法获得，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，经注册机构传递到HBCA。

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，通过如下方式传输给依赖方：

1）依赖方访问HBCA 的证书网站上下载HBCA 根证书，或

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，或

3）HBCA、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，或

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 和最终订户密钥对长度支持1024 位RSA。

6.1.6 公钥参数的生成和质量检查

符合国家密码管理部门的要求。

6.1.7 密钥使用目的

在 HBCA 证书服务体系中的密钥用途和证书类型紧密相关。

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。

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。

6.2.2 私钥多人控制（m 选 n）

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 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。

6.2.3 私钥托管

符合国家主管部门的要求。

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。对于最终订户证书，HBCA 将建议订户对私钥进行备份，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。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 CA 密钥对返回到产品系统中。对归档私钥到了归档保存期，HBCA 将按 CPS § 6.2.10 销毁。

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了 CA 私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

6.2.7 私钥在密码模块的存储

HBCA 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。

6.2.8 激活私钥的方法

6.2.8.1 CA 私钥

HBCA 私钥存放在硬件密码模块中，并且其激活数据按 CPS § 6.2.2 进行分割。当需要使用 CA 私钥时，将硬件密码模块加载并按 5 选 3 的原则输入激活数据的分割。

6.2.8.2 订户私钥

当订户私钥存放在订户计算机的软件密码模块中时，订户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订户授权的情况下其他人员使用订户的计算机。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。

当订户私钥存放存放在诸如 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）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。

6.2.9 解除私钥激活状态的方法

对于存放在软件密码模块中私钥，当软件密码模块被下载、用户退出登录状态、操作关闭或计算机断电时，私钥被解除激活状态。对于存放在硬件密码模块中的私钥，当每次操作后注销计算机，或者把硬件密码模块从读卡器中取出时，私钥成为非激活状态。对于服务器证书，当服务程序下载、系统注销或系统断电后私钥即进入非激活状态。

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

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。

6.2.11 密码模块的评估

由国家密码管理部门负责。

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

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 激活数据的产生与安装

HBCA 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。

订户激活数据是私钥保护口令。HBCA 提供唯一的不可猜测的证书私钥口令。这些私钥口令由 HBCA 根据授权和操作的许可实施批准并且仅发放给授权订户。

6.4.2 激活数据的保护

保存有 HBCA 私钥的激活数据的 5 个 IC 卡分别依据 HBCA 职责分割的要求由 HBCA 5 个不同的可信人员掌管。

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 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。

6.5 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，其它人员不能操作和控制 HBCA 系统；其它普通用户无系统账号和密码。HBCA 系统

部署防火墙、入侵检测系统以及防病毒软件系统，确保系统网络安全。

6.5.2 计算机安全评估

HBCA 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，HBCA 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。

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。

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，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。

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、入侵检测、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 RFC3280 标准。

7.1.1 版本号

X.509v3 证书。

7.1.2 证书扩展项

针对特别的用户，HBCA 签发的证书有可能包含私有扩展项，不能识别私有扩展项的应用、依赖方可以忽略该扩展项。

7.1.3 算法对象标识符

使用 SHA1WithRSAEncryption 算法

算法 OID 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）单位机构证书中应为证书主体单位的标准简称；
c）服务器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）代码签名证书应为负责人的姓名，或者是所属单位的标准简称；

（5）Email 代表电子邮件地址

7.1.5 名称限制

HBCA 签发的证书中的通用名不能使用假名、伪名。

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 RFC3280 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 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

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。审计分内部审计和外部审计。

内部审计是由HBCA 自己组织内部人员组织进行的至少一年一次的审计，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。

外部审计是由信息产业部电子认证服务管理办公室组织的每年一次的评估和检查，审计的内容包括且不限于电子认证业务规则、HBCA 安全策略、及相关管理制度等。

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

8.2评估者的资质

在进行内部评估审计时，HBCA 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。

8.3评估者与被评估者之间的关系

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

8.4评估内容

审计的内容应包括：

- HBCA 支持的证书认证操作规程是否完与本认证业务规则表达一致。
- HBCA 是否实施了相关技术、管理、相关政策和业务规则。

- 审计者或 HBCA 认为有必要审计的其他方面。

8.5 对问题与不足采取的措施

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

8.6 评估结果的传达与发布

审计结果将传达给 HBCA 运营安全管理小组。除非法律明确要求，HBCA 一般不公开审计结果。在必要的情况下，向 HBCA 关联单位（例如注册机构、注册分支机构、受理点）通知审计结果的具体规定将在 HBCA 和关联单位的协议中写明。

9.法律责任和其他业务条款

9.1 费用

9.1.1 证书签发和更新费用

HBCA 数字证书的收费标准按照湖北省物价主管部门批准的收费标准执行。根据实际情况，HBCA 在不高于收费标准的前提下可以根据市场和管理部门规定对证书价格进行适当调整。

9.1.2 证书查询费用

HBCA 目前不对证书查询收取专门的费用。

9.1.3 证书吊销或状态信息的查询费用

证书吊销和吊销列表（CRL）的获取不应收取任何费用。HBCA 有可能根据需要将 OCSP 服务作为增值服务收取费用。

9.1.4 其他服务费用

无规定。

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。

如果由于 HBCA 的原因，造成订户合同无法履行、订户证书无法使用，HBCA 会将有关费用返还给订户。

9.2 财务责任

9.2.1 保险范围

HBCA 保证其具有维持其运作和履行其责任的财务能力。它应该有能力承担对订户、依赖方等造成的责任风险，并依据CPS规定，进行赔偿担保。

9.3 业务信息保密

9.3.1 保密信息范围

HBCA 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；

内部安全管理策略与制度。

- 客户信息

客户的注册信息；

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；

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、申请操作指南等信息是公开的。HBCA 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。

订户数字证书的相关信息可以通过HBCA 目录服务等方式向外公布。

HBCA 在其目录服务器中公布证书的吊销信息，供网上查询。

9.3.3 保护保密信息的责任

HBCA 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。HBCA 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，HBCA 保证不会截取任何证书申请人的资料。

HBCA 应保护证书申请人所提供的，证明其身份的资料。HBCA 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。

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

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。

9.4.4 保护隐私的责任

除非执法、司法方面的强制需要，HBCA 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。

9.4.5 使用隐私信息的告知与同意

HBCA 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 HBCA 或其注册机构：

1）有手写签名的同意和授权文件，并将文件邮寄、快递到 HBCA 或其注册机构，或者

2）将手写签名的同意和授权文件传真到 HBCA ，或者

3）以签名电子邮件的形式同意并授权。

9.4.6 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，HBCA 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，HBCA 及其注册机构也将尽可能地保护客户隐私信息。

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HBCA 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。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。

按本CPS 的规定，所有由HBCA 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HBCA 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HBCA 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。

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：

a) HBCA 遵守《中华人民共和国电子签名法》及《电子认证服务管理办法》等相关法律的规定，接受信产部的业务监督和指导，对 HBCA 所签发的数字证书承担相应的责任和义务。

b) HBCA 保证使用的系统及密码符合国家政策与标准，保证 HBCA 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) HBCA 签发给订户的证书符合 HBCA CPS 规定的所有实质性要求。

d) HBCA 保证证书在有效期内的有效性和可靠性，将向证书订户通报任何已知的、可能在本质上影响证书的有效性和可靠性事件。

e) HBCA 将及时吊销证书，并发布到 CRL 上供订户查询。

f) 证书公开发布后，HBCA 向证书依赖方保证，除未经鉴证的订户信息外，证书

中的其他订户信息均为准确的。

9.6.2 注册机构的陈述与担保

HBCA 的注册机构和下层分支机构在参与电子认证服务过程中的承诺如下：

a) 严格执行 HBCA 中心制定的证书管理和发放策略，服从 HBCA 整体的管理和规范要求；提供给证书订户的注册过程完全符合 HBCA CPS 的所有实质性要求。

b) 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人的信息不一致。

c) 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：

a) 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。

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、真实和准确的，并可供 HBCA 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 HBCA 和注册机构，及时申请采取证书吊销等业务处理。

f) 订户已知其证书被冒用、破解或被他人非法使用时，应按 HBCA CPS 的相关条款及时申请办理吊销其证书业务。

9.6.4 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 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。

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本 CPS §9.6.4。

9.7 担保免责

HBCA 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，HBCA 及注册机构不承担责任。

HBCA 在签发数字证书之前，证书申请者已同意遵守责任书中的各项规定。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，由此得到了 HBCA 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，HBCA 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。HBCA 也不承担任何其他未经授权的人或组织以 HBCA 名义编撰、发表或散布不可信赖的信息所引起的法律责任。

9.8 有限责任

对于由于 HBCA 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，造成了证书订户、依赖方的损失，HBCA 将承担相应的赔偿责任，但这种责任是有限的。

HBCA 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。

9.9 赔偿

对于由如下原因造成的订户或依赖方损失，HBCA 对订户或依赖方进行赔偿，

HBCA 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 HBCA 的原因，使得证书中出现了错误信息；

由于 HBCA CA 私钥的泄漏。

在如下情况，订户对自身原因造成的 HBCA、依赖方损失承担责任，

订户在证书申请中对事实做虚假或错误描述；

在证书申请中订户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；

订户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订户私钥的安全损害、丢失、泄漏、修改或非授权的使用；

订户使用的名字（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 HBCA 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；

而依赖方没有检查证书状态确定证书是否过期或吊销。

如 HBCA 违反了 CPS § 9.8 款条例规定的职责，HBCA 承担赔偿责任（法定或约定免责除外）的赔偿限制如下：

HBCA 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开户费或年服务费的拾倍。

HBCA 只有在 HBCA 证书有效期限内承担损失损害赔偿。

9.10 有效期限与终止

9.10.1 有效期限

HBCA 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，

9.10.2 终止

当新版本的电子认证业务规则正式发布生效时，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

HBCA CPS 的中止（而非更新），意味着 HBCA 认证业务的终止。HBCA 中止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。

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，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

9.12.1 修订程序

本认证业务规则将尽量避免不必要的修改。但不定期地，HBCA 将对本CPS 进行检查、评估，当HBCA 认为应该对本CPS 做出修改时，HBCA 运营安全管理小组成员将对本CPS 及其他相关文档、协议提出修改建议，获得HBCA 运营安全管理小组批准后，由安全管理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、协议经HBCA 法律顾问认可后，报运营安全管理小组批准后正式发布。

9.12.2 通知机制和期限

本 CPS 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 的网站及时公布，对具体个人和单位订户不再另行通知。

9.12.3 必须修改业务规则的情形

当管辖法律、法规、适用标准及操作规范等有重大改变时，必须修改本 CPS 。

9.13 争议处理

如果HBCA、订户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。

9.14 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 HBCA 的业务活动。HBCA 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。

9.15 与适用法律的符合性

HBCA 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。

9.16 一般条款

9.16.1 完整协议

本CPS 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。

9.16.4 强制执行

在 HBCA、注册机构、订户和依赖方之间出现纠纷、诉讼时，胜讼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。

9.16.5 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 HBCA、注册机构无法提供正常的服务时，HBCA、注册机构不承担由此给客户造成的损失。