湖北省数字证书认证管理中心有限公司
证书策略（CP1）

v1.1

发布日期：2025 年 12 月 19 日

生效日期：2025 年 12 月 19 日

湖北省数字证书认证管理中心有限公司

版本修订记录

版本号	状态	修订说明	审核/批准人	生效日期
v1.0	版本发布	新版本发布	公司安全策略委员会	2025 年 3 月 6 日
v1.1	版本发布	内容修订更新	公司安全策略委员会	2025 年 12 月 19 日

目 录

1.引言

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.）（以下简称为“湖北 CA”或“本机构”）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》《电子政务电子认证服务管理办法》的要求以及相关管理规定，提供数字证书申请、受理、签发、接受、更新、变更、撤销、使用等服务，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、企业信息化构建安全可靠的信任环境。

证书策略（CP，Certification Policy）是指定的一组规则,表明了证书在某特定范围内的、和(或)某些具有相同安全需求的应用内的适用程度。

《湖北省数字证书认证管理中心有限公司证书策略（CP1）》（以下简称《湖北 CA 证书策略（CP1）》或“本证书策略”“本 CP”）满足互联网标准组织制定的 RFC3647《互联网 X.509 公钥基础设施-证书策略和证书业务声明框架》，以及中华人民共和国标准 GB/T 26855-2011《信息安全技术公钥基础设施 证书策略与认证业务声明框架》的框架和内容要求。《湖北 CA 证书策略（CP1）》适用范围为湖北 CA 签发的证书，包括个人证书、机构证书、设备证书。具体设定了证书策略、生命周期、使用、依赖和管理的角色、责任与要求，以及各相关主体的职责。为批准、签发、管理和使用证书和相关的可信服务制定业务，提供技术、策略和法律上的要求和规范。

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证书策略（CP1）》，简称《湖北 CA 证书策略（CP1）》。本 CP 对应 OID 为 1.2.156.112681.1.1.1。

1.3.PKI 参与者

本 CP 包含的 PKI 参与者有：电子认证服务机构、注册机构、订户、依赖方以及其他参与者。

1.3.1.电子认证服务机构

电子认证服务机构（Certification Service Provider）是依据《电子签名法》和《电子认证服务管理办法》获得《电子认证服务许可证》向公众提供电子认证业务的机构,一般包含有证书签发机构和订户注册机构。

1.3.2.证书签发机构（CA）

证书签发机构（CA，Certification Authority）是负责签发证书和维护证书状态的实体。

1.3.3.注册机构（RA）

注册机构（RA，Registration Authority）是负责订户的标识和鉴别,批准或拒绝订户的证书申请、撤销申请和挂起申请,发起证书的撤销和挂起的实体。

1.3.4.订户

订户（Subscriber）是与电子认证服务机构签订协议,接受电子认证服务机构提供的服务的实体。订户应能对证书对应的私钥的使用负有法律责任。

1.3.5.依赖方

依赖方（Relying Party）是接受电子认证服务机构的依赖方协议,独立地判断证书的安全性是否满足其应用的安全需求,并验证证书和相应签名的实体。

1.3.6.其他参与者

其他参与者指上述未提及的为湖北 CA 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.适用的证书应用

除湖北 CA 另有约定外，本 CP 中所指的证书是指湖北 CA 签发的保存在订户持有或指定的证书载体中的一类证书。证书载体包括但不限于智能密码钥匙、密码设备。证书适合应用在企业信息化、电子政务和电子商务等领域，用于证明订户在电子化环境中所进行的身份认证和电子签名，以及数据加密等服务。湖北 CA 签发的证书包括个人数字证书、机构数字证书、设备数字证书。

个人数字证书，适用于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；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。

机构数字证书，适用于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。

设备数字证书，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。

1.4.2.限制的证书应用

湖北 CA 发放的数字证书禁止在违反国家法律法规、破坏国家安全或违反湖北 CA 与订户约定的情况下使用，由此造成的法律后果由订户负责。

1.5.策略管理

1.5.1.策略文档管理机构

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

湖北 CA 将对本 CP 进行严格的版本控制，并由湖北 CA 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：430064

网站地址：https://www.hbca.org.cn

电子邮件：cps@hbca.org.cn

1.5.3.决定 CP 符合策略的机构

决定《湖北 CA 证书策略（CP1）》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.CP 批准程序

《湖北 CA 证书策略（CP1）》由本机构安全策略委员会组织 CP 编写小组编写或修订。编写小组完成编写或修订后先形成 CP 评审稿，将评审稿提交安全策略委员会审批。经审批通过后形成正式发布版，在湖北 CA 的网站上对外公布。本 CP 经安全策略委员会审批通过后，从对外公布之日起三十日之内向工业和信息化部备案。

本 CP 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 CP。

电子认证服务机构：Certification Service Provider，依据《电子签名法》和《电子认证服务管理办法》获得《电子认证服务许可证》向公众提供电子认证业务的机构,一般包含有证书签发机构和订户注册机构。

证书签发机构（CA）：Certification Authority，负责签发证书和维护证书状态的实体。

注册机构（RA）：Registration Authority，负责订户的标识和鉴别,批准或拒绝订户的证书申请、撤销申请和挂起申请,发起证书的撤销和挂起的实体。

证书策略（CP）：Certification Policy，指定的一组规则,表明了证书在某特定范围内的、和(或)某些具有相同安全需求的应用内的适用程度。

电子认证业务规则（CPS）：Certification Practice Statement，电子认证服务机构对其签发、管理、撤销和更新证书的相关措施和实施行为的一份声明。

证书撤销列表（CRL）：Certificate Revocation List，由电子认证服务机构维护的,包含由于各种原因(例如:私钥泄露、证书中的信息发生改变)在有效期内被撤销的证书的列表。

在线证书状态协议（OCSP）：Online Certificate Status Protocol。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，由国家认可的，具有权威性、可信性和公正性的第三方证书认证机构（CA）进行电子签名的一个可信的数字化文件。

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：接受电子认证服务机构的依赖方协议,独立地判断证书的安全性是否满足其应用的安全需求,并验证证书和相应签名的实体。

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.信息库发布与管理

2.1.信息库

本机构提供一个对外公开的信息库，面向订户及依赖方提供信息服务。提供的信息服务包括但不限于以下内容：CP、CPS、证书、证书状态和 CRL。本机构负责管理和维护此信息库。

2.2.认证信息的发布

本机构通过公司官网发布或者通过其他方式提供 CP、CPS。本机构提供公开方式或定制方式向订户及依赖方提供 CRL 下载服务或在线证书状态查询服务。

2.3.发布的时间或频率

本机构的 CP、CPS 按照内部批准程序不定期修订并发布。CRL 通常每 24 小时发布一次。

2.4.信息库访问控制

对于公开发布的 CP、CPS 等信息以及 CRL 下载或在线证书状态查询服务，允许订户或依赖方通过本机构的官方渠道（例如：公司官网、定制化服务）获取。

本机构的安全访问控制机制确保只有经过授权的人员才能修改信息库中的信息。

本机构在必要时可自主选择是否实行信息的权限管理，以确保 PKI 参与相关方的实际权益。

3.标识与鉴别

3.1.命名

3.1.1.名称类型

本机构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。

本机构签发的证书符合 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，可追溯到证书主体中的个人、机构或设备的身份。

3.1.3.订户的匿名或伪名

在本机构的证书服务体系中，订户不宜使用匿名和伪名。

3.1.4.解释不同名称形式的规则

本机构签发的数字证书应符合 X.509 标准，甄别名（DN）格式遵守 X.500 标准。

3.1.5.名称的唯一性

本机构签发给某个实体的证书，其主题甄别名，在本机构信任域内是唯一的。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

本机构签发的证书不包含任何商标或者可能对其他机构造成侵权的信息。

3.2.初始身份认证

3.2.1.证明拥有私钥的方法

本机构通过使用经数字签名 PKCS#10 格式的证书请求，或其他本机构认可的方法，验证订户拥有私钥。

3.2.2.组织机构身份的鉴别

收到组织机构订户证书申请材料后，应对订户的身份真实性及其它申请材料进行鉴别，鉴别方式可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对身份证件信息进行比对。鉴别内容包含但不限于以下内容：

- 订户提交的组织身份信息，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。
- 经办人的授权证明材料，经办人个人身份证明材料。
- 申请设备证书时，需提交权属证明材料。

鉴别审核通过后，本机构按照相关法律法规的要求妥善保存订户申请材料，保存订户申请材料可以是纸质或电子数据形式。

本机构保留根据最新国家政策法规的要求更新组织机构身份鉴别方法与流程的权利。

3.2.3.个人身份的鉴别

收到个人订户证书申请材料后，应对订户的身份真实性及其它申请材料进行鉴别，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。

鉴别审核通过后，本机构按照相关法律法规的要求妥善保存订户申请材料，保存订户申请材料可以是纸质或电子数据形式。

本机构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.没有验证的订户信息

订户提交验证文件以外的信息视为没有验证的订户信息。

3.2.5.授权确认

被订户授权办理证书的经办人，需审核其身份资料、授权证明和资格等信息。

3.3.密钥更新请求的标识与鉴别

3.3.1.常规密钥更新的标识与鉴别

在常规密钥更新中，通过订户使用当前有效私钥对密钥更新请求进行签名，本机构使用订户原有公钥验证确认签名或采用安全授权认证的方式来进行订户身份标识和鉴别。本机构也可以使用初始身份验证相同的流程进行标识与鉴别。

3.3.2.撤销后密钥更新的标识与鉴别

证书撤销后，不能进行密钥更新。

3.4.撤销请求的标识与鉴别

订户申请吊销时的身份标识和鉴别使用原始身份验证相同的流程，按照本 CP3.2.2.、3.2.3.、3.2.5.节中的要求对订户进行身份鉴别。

如果订户没有履行《湖北 CA 电子认证业务规则》、《湖北 CA 数字证书服务协议》所规定的义务，本机构撤销证书时，不需要对订户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，本机构将以司法机关提供的书面撤销请求文件作为鉴别依据。

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、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 CP 所规定的要求，向本机构提交证书申请资料，包括相关的身份证明材料。本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。

1、订户责任：

- 必须明确表示同意数字证书服务协议中的内容，按要求填写本机构的数字证书申请资料，提供真实、有效、完整的身份信息。
- 配合本机构完成对身份信息的采集、记录和审核。

2、本机构责任：

- 本机构参照本 CP3.2.节中的要求，对订户的身份信息进行采集、记录和审核。
- 审核通过后，本机构向订户签发数字证书。

3、注册机构的责任：

- 注册机构应参照本 CP3.2.节所述的要求，对订户的身份信息进行采集、审核和记录。审核通过后，向本机构提交证书申请，由本机构向订户签发证书。
- 注册机构必须接受本机构和国家相关机构的监督管理和审计。
- 注册机构应当按照本机构的要求，向本机构提交身份鉴别材料。

根据《中华人民共和国电子签名法》的规定，订户未向本机构提供真实、完整和准确的信息，或者有其他过错，给本机构、依赖方造成损失的，应承担相应的法律责任和经济赔偿。

4.2.证书申请处理

4.2.1.执行标识与鉴别功能

本机构须按照本 CP3.2.节要求对申请者身份进行标识和鉴别。

4.2.2.证书申请批准和拒绝

收到申请者的申请后，按照本 CP 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 CP 所规定的身份鉴别流程且鉴别结果为合格，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别，将拒绝申请者的证书申请，并通知申请人鉴证失败，同时告知申请者鉴别失败的原因（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

依据鉴别结果，作出批准或拒绝申请的决定后，将在 1 个工作日内处理证书申请。

能否在上述时间期限内处理证书申请取决于证书申请人是否真实、完整、准确地提交了相关信息和是否及时地响应了本机构的管理要求。

4.3.证书签发

4.3.1.证书签发中电子认证服务机构的行为

本机构在批准证书申请之后，将签发证书。证书的签发意味着电子认证服务机构完全正式地批准了证书申请。

4.3.2.电子认证服务机构对订户的通告

本机构告知订户证书的签发结果和获取证书的方式，可通过系统提示、消息推送或本机构认为其他安全的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

证书签发完成后，订户通过本 CP 所通告的方式获取证书，在订户发生以下任意一种行为后，将被视为同意接受证书：

- 订户支付电子认证服务费且本机构已完成订户身份核验及证书签发并已告知证书获取方式，即视为已经接受证书。
- 订户将证书应用于对应的电子签名或其他密码运算时起，即视为已经接受证书。
- 本机构将证书获取通知发送给订户后，在 24 小时内订户未表示拒绝。

订户在提交了证书申请并接受了本机构所签发的证书后，均视为已经同意遵守与本机构、依赖方有关的权利和义务的条款。

4.4.2.CA 对证书的发布

对于订户证书，本机构将根据订户的意愿采取适当形式发布，订户没有要求发布的，本机构将不发布订户证书。

4.4.3.就签发证书 CA 对其他实体的通告

对于签发的证书，本机构不对其他实体进行通告。

4.5.密钥对和证书的使用

4.5.1.订户私钥和证书的使用

订户在提交了证书申请并接受了本机构所签发的证书后，均视为已经同意遵守与本机构、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。

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。未按规定用途使用造成的损失由订户自行承担。

4.5.2.依赖方公钥和证书的使用

依赖方只能在约定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）。当依赖方接收到经数字签名的信息后，应该：

1、获取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，确认该证书没有被撤销；

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，在验证数字签名时，依赖方应准确知道什么数据已被签名。在公钥密码标准里，标准的签名信息格式被用来准确表示签名过的数据。

以上任何一个环节失败，依赖方应该拒绝接受签名信息，未经验证接受签名信息导致损失的，由依赖方自行承担。

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，然后使用该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

在接收到订户或其授权代表提交的证书更新请求时，本机构对证书及密钥进行更新。

4.6.2.请求证书更新的主体

订户或其授权代表可以请求证书更新。

4.6.3.证书更新请求的处理

同本证书策略 4.2.2.。

由于订户未及时办理证书更新而导致原证书过期或无法使用，本机构不承担任何责任。

4.6.4.颁发新证书时对订户的通告

同本证书策略 4.3.2.。

4.6.5.构成接受更新证书的行为

同本证书策略 4.4.1.。

4.6.6.CA 对更新证书的发布

同本证书策略 4.4.2.。

4.6.7.就签发证书 CA 对其他实体的通告

同本证书策略 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

证书密钥更新是指当证书到期、丢失、密钥已经或怀疑发生泄漏、被窃取、被篡改或者其他需要更换密钥的时候，订户可以选择密钥更新服务。

4.7.2.请求证书密钥更新的主体

同本证书策略 4.6.2.。

4.7.3.证书密钥更新请求的处理

同本证书策略 4.6.3.。

4.7.4.颁发新证书时对订户的通告

同本证书策略 4.3.2.。

4.7.5.构成接受密钥更新证书的行为

同本证书策略 4.4.1.。

4.7.6.CA 对密钥更新证书的发布

同本证书策略 4.4.2.。

4.7.7.就签发证书 CA 对其他实体的通告

同本证书策略 4.4.3.。

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。本机构在对申请者递交的资料进行验证确认后，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主体信息而签发新证书的情形。当证书主体身份信息发生改变，而影响证书内容时，证书订户有义务向本机构报告并申请证书变更，将原证书撤销后重新签发新证书。

4.8.2.请求证书变更的主体

同本证书策略 4.6.2.。

4.8.3.证书变更请求的处理

同本证书策略 4.6.3.。

4.8.4.颁发新证书时对订户的通告

同本证书策略 4.3.2.。

4.8.5.构成接受变更证书的行为

同本证书策略 4.4.1.。

4.8.6.CA 对变更证书的发布

同本证书策略 4.4.2.。

4.8.7.就签发证书 CA 对其他实体的通告

同本证书策略 4.4.3.。

4.9.证书撤销和挂起

4.9.1.证书撤销的情形

证书撤销分为主动撤销和被动撤销，主动撤销是指订户主动申请撤销其数字证书，注册机构审核申请后撤销其证书。被动撤销是指本机构确认用户违反本CP、电子认证服务协议、证书主体消亡的，则撤销数字证书。

本机构没有义务公开证书被撤销的原因。

一、发生下列情形之一的，订户应当主动申请撤销数字证书：

1、数字证书私钥被泄漏、窃取、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 CP、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，本机构可以强制撤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 CP、其它协议、法规或法律所规定的责任和义务；

3、订户不能履行电子签名行为的；

4、发现并证实其证书没有根据本 CP 要求的程序而签发的；

5、数字证书的安全性得不到保证；

6、法律、行政法规规定的其他情形。

本机构有权不公开某一张证书被撤销的原因。

4.9.2.请求证书撤销的主体

根据不同的情况，订户、本机构、国家法律部门、政府主管部门及其它公共权力部门可以请求撤销最终用户证书。

4.9.3.撤销请求的流程

证书撤销请求的处理采用与原始证书签发相同的过程。

4.9.4.撤销请求宽限期

如果出现私钥泄露等事件，撤销请求必须在发现泄露或有泄露嫌疑 8 小时内提出。其他撤销原因的撤销请求必须在 48 小时内提出。

4.9.5.CA 处理撤销请求的时限

本机构在受理订户撤销请求后立即处理，24 小时内撤销符合条件的证书，并按照 CRL 的发布频率发布到证书撤销列表。

4.9.6.依赖方检查证书撤销的要求

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、证书状态查询等。

本机构将在公司官网（www.hbca.org.cn）上提供证书撤销列表、在线证书状态查询方法。

4.9.7.CRL 发布频率

本机构每 24 小时更新和公布一次证书撤销列表（CRL）。

本机构根据情况，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

CRL 发布的最大滞后时间为证书撤销列表生成后不超过 24 小时。

4.9.9.在线状态查询的可用性

本机构提供证书状态查询服务。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

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.撤销信息的其他发布形式

无其他途径。

4.9.12.密钥损害的特别要求

除本 CP4.9.1.节中规定的情况外，订户或本机构发现证书密钥受到安全损害时应立即撤销证书。

4.9.13.证书挂起的情形

不提供证书挂起服务。

4.9.14.请求证书挂起的实体

无此情形。

4.9.15 证书挂起和恢复（解挂）的流程

无此情形。

4.9.16 挂起的期限限制

无此情形。

4.10.证书状态服务

4.10.1.操作特征

本机构通过 CRL、OCSP 提供证书状态查询服务。

4.10.2.服务可用性

同本证书策略 4.9.9.。

4.10.3.可选特征

无此情形。

4.11.订购结束

订户出现下列情形时说明该订户的证书服务订购已结束：

- 证书到期后没有进行更新。
- 证书到期前被撤销。
- 证书到期前提出终止服务。

4.12.密钥托管与恢复

4.12.1.密钥托管与恢复的策略与行为

订户的签名密钥对在订户持有或指定的证书载体中产生,证书载体包括但不限于智能密码钥匙、密码设备、密码模块。加密密钥对由密钥管理中心生成。

密钥恢复是指订户加密密钥对的恢复,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:用户密钥恢复和司法密钥恢复。

4.12.2.会话密钥的封装与恢复的策略与行为

利用非对称加密算法对会话密钥进行加密封装，以构建数字信封。会话的发起方使用接收方的公钥对会话密钥进行加密，接受方用自己的私钥解密并恢复会话密钥。

5.设施、管理和操作控制

5.1.物理控制

5.1.1.场所区域和建筑

本机构电子认证业务运营场所位于湖北省武汉市武昌区华中小龟山金融文化公园 9 栋。湖北 CA 机房严格按照分层建设、多级管理的要求布局。建设过程中将每一个层次建设为一道安全的屏障，并划分为相对独立的安全区域。需要进入机房不同层次区域的人员必须得到相应的授权方可进入。

机房按照国家相关标准建设，已通过国家密码管理部门的安全性审查。核心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机房区域的常规入口。

5.1.2.物理访问

为了保证电子认证系统的安全，机房内各区域采取了一定的隔离、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保护机房物理安全。

物理访问控制包括如下几个方面：

1、每一道门的每次进出都有门禁记录作为审计依据；

2、门禁系统采用身份识别卡和生物识别双重认证的控制方法，控制每道门的进入，进入需要两人通过认证，退出需要一人通过认证；

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

机房的供电系统提供包括机房区域内的动力、照明、监控、通讯、维护等用电。供电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。

使用不间断电源（UPS）来保证供电的稳定性和可靠性。采用双电源，在单路电源发生故障时，可以维持系统正常运转。

根据机房环境及设计规范要求，湖北 CA 机房使用机房专用空调,进行温度的调控，并配备湿度控制设备来调控机房湿度。

5.1.4.水患防治

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，防止水患发生降低水患影响。

5.1.5.火灾防护

湖北 CA 机房的消防报警系统和灭火系统均通过公安消防部门或具备消防检测资质的第三方机构的消防检测。

在湖北 CA 机房各区域内均设置了烟、温感探测器，并配置了独立的气体灭火装置。

5.1.6.介质存储

本机构对储存关键数据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，只允许授权人员访问，并防止这些介质受到意外损坏（如水、火灾和电磁破坏）。

5.1.7.废物处理

当本机构存档的敏感数据或密钥已不再需要或存档的期限已满时，应当由相应的管理人员将这些数据进行销毁。纸质记录必须切碎或烧毁，保存在磁盘或其他存储介质中的，以不可恢复原则进行销毁处理。

5.1.8.异地备份

本机构对关键系统数据、审计日志数据和其他敏感信息进行日常备份，并在定期归档后进行异地保存，这些备份信息保存在湖北 CA 建筑物以外的安全的地方。

5.2.过程控制

5.2.1.可信角色

本机构可信角色至少包括：

- 系统管理维护人员
- 密钥和密码设备管理人员
- 安全管理人员
- 系统审计人员
- 身份鉴别、材料验证和客服人员

5.2.2.每项任务需要的人数

本机构确保单人不能接触、备份、恢复、更新、废止本机构存储的 CA 证书对应的私钥。至少需要三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 CA 密钥的操作。

本机构对每个角色所承担的职责和任务都有明确的分工，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

所有本机构的可信角色人员，在进入湖北 CA 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或账号进行身份鉴别。本机构将独立完整地记录其所有的操作行为。

5.2.4.需要职责分割的角色

为保证系统安全，遵循可信角色职责分割的原则，即 CA 机构的可信角色由不同的人员承担。至少包括：

- 系统管理维护人员
- 密钥和密码设备管理人员
- 安全管理人员
- 系统审计人员
- 身份鉴别、材料验证和客服人员

5.3.人员控制

5.3.1.资格、经历和无过失要求

本机构所有的员工必须与湖北 CA 签订保密协议。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。本机构确立了流程管理和规则，员工受

到劳动合同、保密协议和规章制度的约束，不得泄露湖北 CA 证书服务体系的敏感信息。

本机构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。湖北 CA 可信任员工的背景调查由人事部门负责，如有需要，可与有关的政府部门和调查机构合作，完成对本机构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，本机构对雇佣的人员先进行背景调查。在成为本机构的可信人员前，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。

本机构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，本机构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

本机构对员工进行综合性的培训，培训内容包括：

- 职业行为规范及岗位职责
- 安全管理要求及公司管理制度
- 保密制度及相关法律法规
- PKI 及应用
- 湖北 CA 的产品与服务
- 其他需要进行的培训

5.3.4.再培训周期和要求

本机构根据业务需要安排。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，本机构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

本机构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

对不属于本机构内部的工作人员，但从事本机构有关业务的人员等独立签约者，本机构的统一要求如下：

1、人员档案进行备案管理；

2、具有相关业务的工作经验；

3、必须接受本机构的监督与管理；

4、必须签订《保密协议》，使其能够严格遵守本机构的管理规范。

5.3.8.提供给员工的文档

为使得系统正常运行，本机构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

本机构须记录与 CA 和 RA 运行相关的事件。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。主要包括：

- 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）
- 认证系统日常运行产生的日志记录文件
- 进出敏感区域的工作记录
- 可信角色人事变动的相应记录
- 其它按规定需要记录的内容

5.4.2.处理日志的周期

本机构每月对日志进行审查，并对审查的日志进行归档。

5.4.3.审计日志的保存期限

本机构审计日志保存期限不低于 5 年。

5.4.4.审计日志的保护

本机构执行严格的管理，确保只有本机构授权的人员才能对审计日志进行相应操作。日志处于严格的保护状态，严禁在未授权的情况下被访问、修改或删除。

5.4.5.审计日志备份程序

对于电子认证系统的审计日志，本机构定期进行备份。

5.4.6.审计日志收集系统

电子认证系统审计日志收集系统在证书签发和证书注册系统内部。

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，本机构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

本机构定期对系统采用漏洞扫描等方式进行脆弱性评估，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

本机构归档记录的类型见本 CP5.4.1.节。

5.5.2.归档记录的保存期限

本机构所有归档文件的保存期一般规定为五年。

本机构订户证书和订户在办理证书业务时提交的资料一般归档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

本机构对各种电子、磁带、纸质形式的归档文件，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

所有归档的文件和数据保存在本机构内部安全存储区域，部分归档文件还将异地保存其备份。归档文件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，才能对归档文件进行读取操作。本机构在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

5.5.5.记录时间戳要求

本机构对每项日志有时间记录。

5.5.6.归档收集系统

湖北 CA 电子认证系统的归档信息全部由本机构内部工作人员或通过具有安全控制措施的内部系统，采用人工或自动方式产生和收集，并且由具备相关权限的人员进行分类管理。

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 CP6.3.2 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，湖北 CA 将启动 CA 密钥更新流程。按照 CA 密钥相关管理和操作规范产生新的 CA 密钥替换原有 CA 密钥，并确保新旧 CA 密钥的平滑过渡。

5.7.损害与灾难恢复

5.7.1.事故和损害处理程序

本机构制定了一系列应急预案，对可能发生的事故和处理程序进行了定义。当发生相关事故时，本机构将按照相应急预案进行处理。

5.7.2.计算资源、软件和/或数据的损坏

本机构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，当出现计算资源、软件和/或数据的损坏时在最短的时间内恢复被损坏的资源、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，本机构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，并立即前往本机构申请注销其证书；

2、当本机构证书订户的实体私钥受到损害时，本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、当本机构的 CA 证书出现私钥损害时，本机构将吊销 CA 证书并及时通知依赖方，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

湖北 CA 电子认证系统采取软硬件冗余或集群部署的方式来提升系统的高可用性和容灾能力。同时对关键核心数据进行异地备份，在物理场地或系统数据出现重大灾难时能够根据需要尽快恢复其业务。

5.8.CA 或 RA 的终止

当湖北 CA 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》、《电子政务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

根 CA 密钥对由本机构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。生成和保存 CA 根密钥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.订户密钥对的产生

订户的签名密钥对应使用国家密码主管部门许可的密码模块产生。

订户的加密密钥对是由国家密码管理部门许可的，湖北 CA 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。

6.1.2.私钥传送给订户

订户的签名私钥由订户自己的密码钥匙或密码设备产生时，私钥由订户自行保管，不存在传送的情形；由本机构协助订户产生时，私钥由本机构通过安全方式传递给订户，安全方式包括但不限于面对面、密码信封、安全网络通道等方式。订户加密私钥由 KMC 产生，通过安全通道从 KMC 传递到订户的密码钥匙或密码设备中。

如果本机构获知订户私钥被非订户本身或非订户授权人员获得，本机构将撤销该私钥所对应的公钥证书。

6.1.3.公钥传送给证书签发机构

订户的签名证书公钥经注册机构通过安全通道传递到湖北 CA 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湖北 CA 数字证书签发系统。

从 RA 到 CA 以及从 KMC 到 CA 的传递过程中，采用国家密码管理部门许可的通讯协议及密码算法，保证了传输中数据的安全。

6.1.4.CA 公钥传送给依赖方

对于本机构的 CA 公钥，可通过包含但不限于如下四种方式传送给依赖方：

1、依赖方可以通过本机构的网站下载 CA 证书；

2、本机构、注册机构到依赖方业务系统现场将 CA 证书安装到业务系统中；

3、本机构、注册机构通过电子邮件将 CA 证书传输给依赖方；

4、本机构、注册机构分发给依赖方的软件中绑定、包含有 CA 证书。

6.1.5.密钥的长度

本机构遵从国家法律法规、政府主管机构等对密钥长度的明确规定和要求。

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

在湖北 CA 证书服务体系中的密钥用法和证书类型紧密相关。

CA 证书的密钥使用目的包括签发证书和 CRL。

订户证书依据应用场景配置密钥用法及增强型密钥用法。

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

本机构电子认证系统的密码设备使用国家密码管理部门许可的产品，密码设备的标准和安全级别符合国家规定的要求。本机构制定了专门的密钥安全管理策略，从密码设备的管理和使用以及密钥全生命周期的管理进行了详细规定。

存储订户证书私钥的密码模块应使用国家密码管理部门许可的产品，密码模块的标准和安全级别应符合国家规定。

6.2.2.私钥多人控制

本机构电子认证系统根 CA 私钥存放在符合安全要求的密码设备中，该密码设备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 卡分别由多名本机构的可信雇员持有（称为密钥分管者），保存在保险柜内部分隔的保险盒中。当要操作使用 CA 私钥时（如生成、更新、销毁、备份和恢复等），需要按照密码设备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 卡通过密码设备验证后才能由授权人员进行相应操作。

订户的私钥由订户控制。

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订户自行妥善保管。

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

6.2.4.私钥备份

本机构对 CA 私钥通过专门的智能密码钥匙或 IC 卡进行备份，备份操作将按照本 CP §6.2.2 私钥多人控制的机制进行。

本机构不备份订户的签名密钥，签名私钥由订户自行妥善保管；KMC 备份托管加密私钥，备份数据以密文形式存在。

6.2.5.私钥归档

当本机构的 CA 私钥对到期后，将归档保存 5 年。

本机构不对订户的签名私钥进行归档。

KMC 可以对过期的订户加密私钥进行归档，归档加密私钥以密文形式保存。

6.2.6.私钥导入、导出密码模块

本机构的 CA 私钥在硬件密码模块内生成，保存和使用。本机构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，本机构对 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密码模块之间传送。

订户的签名私钥由订户使用符合安全要求的密码模块生成，保存和使用，无法导出。订户的加密私钥通过安全信道以密文形式导入订户的密码模块中。

6.2.7.私钥在密码模块的存储

本机构采用国家密码管理部门认可的密码设备或密码模块，这些设备或模块内置的协议、算法等均符合国家密码管理部门的标准要求。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 私钥安全存储在硬件密码设备中。CA 私钥必须按照本 CP6.2.2.节所述的私钥由多人控制的方式先生成然后激活，激活后只能由湖北 CA 电子认证系统调用。

6.2.8.2.订户私钥

订户私钥被 PIN 码（口令）或其他安全形式的激活数据所保护，通过 PIN 码（口令）等激活数据验证后才能使用私钥。

订户应采用合理的措施保护 PIN 码（口令）等形式的密钥激活数据，防止密码模块内的私钥被窃取或非法使用。

6.2.9.解除私钥激活状态的方法

对于本机构的 CA 私钥，当存储 CA 私钥的硬件密码设备断电时，私钥进入非激活状态。

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。

6.2.10.销毁私钥的方法

本机构的 CA 私钥需要销毁时，应按照本 CP6.2.2.节的私钥多人控制方式由多名密钥分管者通过密码设备验证后由具有销毁密钥权限的管理员进入密码机管理程序，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钥匙或密码设备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，本机构不承担任何责任。

6.2.11.密码模块的评估

本机构使用通过国家密码管理部门检测认证的硬件密码设备存储 CA 私钥。密码设备符合国家有关标准。密码设备采用国家密码管理部门许可的分组密码算法和非对称密码算法，密钥采取分层结构逐层提供保护。

本机构提供给订户使用的密码模块（如：智能密码钥匙）均为通过国家密码管理部门检测认证的产品，技术指标符合国家有关标准。非本机构提供给订户的密码模块由订户评估，并对其安全性和合规性负责。

6.3.密钥对管理的其他方面

6.3.1.公钥归档

订户的证书中包含对应的公钥。本机构定期对过期的订户证书进行归档。

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。

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，并分割保存在多个智能密码钥匙或 IC 卡中，需通过服务器密码机内置的接口或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），或通过其他安全认证方式激活。激活数据由订户在初始化密码模块或初次使用密钥时设置。订户应保证设置的激活数据满足一定的长度和复杂度的要求并定期修改。

6.4.2.激活数据的保护

保存有 CA 私钥的激活数据的多个智能密码钥匙或 IC 卡分别由多名本机构的可信管理人员掌管，且安全存放在保险柜内的独立上锁的保险盒内。

订户使用口令或 PIN 码形式的激活数据来保护私钥时，应由订户自己妥善保管好其口令或 PIN 码，防止激活数据泄露或被窃取。订户使用其他形式的激活数据（如：生物特征）来保护私钥时，订户也应注意防止其激活数据被盗用或窃取。

6.4.3.激活数据的销毁

本机构的 CA 私钥不再被使用或者 CA 证书到期或被吊销后，并且确定 CA 私钥必须被销毁时，应将密码设备中存储的 CA 私钥清除。同时，所有用于激活私钥的智能密码钥匙或 IC 卡等也必须被销毁。所有销毁操作必须在安全管理人员和密钥管理人员的监督下执行。

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：

用于保护私钥的激活数据（如：PIN 码、口令等），建议订户根据业务应用和使用环境的安全需要定期修改。

6.5.计算机安全控制

6.5.1.特别的计算机安全技术要求

本机构电子认证服务系统的数据文件和设备由专职管理员维护管理，未经授权，其他人员不能访问、操作和控制本系统。系统部署了防火墙、入侵防御系统、漏洞扫描系统、防病毒系统，确保系统和网络环境安全。本系统采用增加冗余资源的方法，提高系统的可靠性。另外制定了确保系统安全运行的管理制度和操作流程，专职授权人员严格按照相关制度和流程执行系统的管理和维护操作。

6.5.2.计算机安全评估

本机构电子认证服务系统已经通过国家密码管理部门的安全性审查，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

本机构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

本机构采取有效的安全管理控制机制来控制和监控电子认证系统的安全运行和正确配置，预防系统被入侵并防止未经授权的修改。安全管理控制机制包括各种安全策略、管理制度、工作流程以及相关的技术控制方式。

6.6.3.生命周期的安全控制

本机构电子认证系统从设计到实现，始终确保系统的安全性。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国家密码管理部门鉴定，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。系统正式上线前通过了国家密码管理部门组织的安全性审查。本机构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。采用了防火墙、防病毒系统、入侵防御、漏洞扫描等网络安全防护系统和设备保障系统网络的安全。

7.证书、证书吊销列表和在线证书状态协议

7.1.证书

本机构签发的证书均符合 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，本机构签发的证书除使用 IETF RFC5280 中定义的证书扩展项外，还支持自定义（非关键）扩展项。

7.1.3.算法对象标识符

本机构签发的证书中使用的算法对象标识符，符合国家密码主管部门批准的算法对象标识符。

7.1.4.名称形式

本机构数字证书中的主体 Subject 的 X.500 DN 是 C=CN 命名空间下的 X.500 目录唯一名字，各属性的编码优先使用 UTF8String 或 PrintableString。

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

C=CN

O=**

O=**

OU=**

OU=**

CN=**

1、C（Country）应为 CN，表示中国；

2、O（Organization）

a）代表证书主体所在的组织机构；

b）CA 机构自定义的信息标识，用于标识证书主体的某一特征。

3、OU（Organization Unit）

a）代表证书主体所在的部门；

b）CA 机构自定义的信息标识，用于标识证书主体的某一特征。

4、CN（Common Name）中的内容分为 3 种：

a）个人证书中应为证书主体的姓名或其他的个人唯一标识；

b）机构证书中应为证书主体单位的标准全称或简称或机构唯一标识；

c）设备证书应为证书主体的域名或者 IP 地址或者其他编码。

5、若证书 DN 中存在 E 项，应为证书主体的有效电子邮件地址。

6、证书主体 DN 还可根据需要包含 X.500 相关标准的其他属性。

7.1.5.证书策略对象标识符

当本机构签发的证书中包含证书策略扩展项时，该扩展项中的对象标识符与本 CP 的对象标识符相对应。

7.2.证书吊销列表

7.2.1.版本号

本机构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。

8.一致性审计和其他评估

本机构定期或不定期进行一致性审计和运营评估，检查和监督是否按照国家相关法律法规、《湖北 CA 电子认证业务规则》、及本 CP 的要求依法依规开展电子认证服务业务，以保证证书服务的可靠性、安全性和可控性。

8.1.审计或评估的频度和情形

内部审计或评估是由本机构组织内部审计人员进行的至少一年一次的定期审计。如果出现特殊情况则单独启动审计或风险评估，引发评估或审计事件的特殊情况包括疑似或真实的敏感信息泄密、客户反馈异常、重大的系统变更等。审计的结果可供本机构 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 本机构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.审计或评估人员的资质

内部审计或评估人员要求具备认证机构、信息安全审计的相关知识。熟悉《湖北 CA 电子认证业务规则》及本 CP 的相关内容，具备计算机、网络、信息安全等方面的知识和实际工作经验。

外部审计或评估人员的资质，由主管部门确定。

8.3.评估者与被评估者的关系

评估者应是与被评估者无任何业务、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。评估者应以独立、公正、客观的态度对被评估的对象进行评估。

8.4.审计或评估的内容

本机构内部审计或评估的内容包括但不限于：物理环境安全与控制、系统和网络安全与控制、密钥管理操作、证书生命周期管理、业务规则执行情况等。

外部审计或评估的内容由主管部门确定。

8.5.对问题与不足采取的措施

如果在审计或评估过程中发现执行规范存在问题或不足，本机构将根据审计或评估报告的检查结果，制定整改措施并实施整改，由湖北 CA 安全策略委员会监督执行，接受整改后的再次审计或评估。

8.6.审计或评估结果的传达与发布

审计或评估结果将传达给湖北 CA 安全策略委员会。

除非法律明确要求，本机构一般不对外公开审计或评估结果。

9.业务和法律事务

9.1.费用

9.1.1.证书签发和更新费用

本机构数字证书价格参照市场行情及证书的实际应用需要进行合理定价。

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，本机构暂不收取查询费用。

9.1.3.证书撤销或状态信息的查询费用

查询证书是否撤销，本机构暂不收取此项费用，但保留对此项服务收费的权利。对于在线证书状态查询（OCSP）与依赖方或订户在协议中约定。

9.1.4.其他服务费用

本机构可根据请求者的要求，订制各类服务，具体服务费用由本机构与订户或依赖方另行约定。

9.1.5.退款策略

在实施证书操作和签发证书的过程中，本机构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，本机构将不办理退证、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，本机构将不退还剩余时间的服务费用。

9.2.财务责任

本机构保证具有维持运作和履行其责任的财务能力。本机构有能力承担对订户、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；

对于本机构来说，保密信息包括但不限于以下方面：

1、订户的私钥是保密的；

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，由本机构掌握的，除作为证书、CRL、认证策略被明确发布之外的个人和公司的信息需要保密。

本机构不保存任何证书应用系统的交易信息。

除非法律明文规定，本机构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。湖北 CA 在目录服务器中公布的证书信息及其状态信息，不属于保密信息。

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，湖北 CA 保留追究责任的权利。

9.3.3.保护保密信息的责任

本机构具备严格的管理制度、流程和技术手段用以保护客户机密信息。

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，本机构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》有关订户个人信息保护条款的完整内容见本机构官方网站（https://www.hbca.org.cn/）公布的《个人信息保护政策》。

本机构尊重所有订户和他们的隐私，个人隐私信息保密方案遵守现行法律和政策规定。任何订户选择使用本机构的证书服务，就表明已经同意接受本机构的个人信息保护制度。

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、以及该证书的状态信息等，不认为是隐私信息。

9.4.4.保护隐私的责任

本机构和授权的注册机构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。但当本机构在法律、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 CP 中具有保密性质的信息时，本机构可以按照法

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，本机构无须承担任何责任。

9.4.5.使用隐私信息的告知与同意

本机构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，本机构没有告知订户的义务，也无需得到订户的同意。

本机构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，本机构将依法提供订户个人相关信息：

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，本机构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

当本机构在国家法律、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，本机构按照法律、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，本机构无须承担任何责任。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和订户协议约定处理。

9.5.知识产权

除非额外声明，本机构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。本机构

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。

本机构制订并发布的 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本机构。

9.6.陈述与担保

除非本机构作出特别约定，若本 CP 的规定与本机构制定的其他相关规定、指导方针相互抵触，订户必须接受本 CP 的约束。在本机构与包括订户在内的其他方签订的仅约束签约双方的协议中，对协议中未约定的内容，视为双方均同意按本 CP 的规定执行；对协议中不同于 CP 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

本机构在提供电子认证服务活动过程中的承诺如下：

1、本机构遵守《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、本机构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、本机构签发给订户的证书符合本 CP 的所有实质性要求。

4、本机构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、本机构将及时撤销证书，并发布到 CRL 上供订户查询。

6、证书公开发布后，本机构向证书依赖方承诺，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

本机构授权的注册机构在参与电子认证服务过程中的承诺如下：

1、遵循本机构制订的服务受理规范、系统运作规范和管理规范，根据本 CP

和本机构公布的规范提供相应的证书服务，提供给证书订户的注册过程完全符合本机构既定规则的所有实质性要求。

2、在本机构生成证书时，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 CP 的规定，及时响应并向本机构提交订户证书申请、撤销、更新等服务请求。

9.6.3.订户的陈述与担保

订户一旦接受本机构签发的证书，就被视为向本机构、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 CP 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，可供本机构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，订户应立刻通知本机构和注册机构，申请采取撤销等处理措施。

6、订户已知其证书被冒用、破解或被他人非法使用时，应及时通知本机构撤销其证书。

7、证书将按本 CP 的规定，只用于经过特定的或其它合法的使用目的。

8、一旦证书被撤销后，订户将不能再使用该证书。

9、订户在取得证书后应及时确认证书信息无误。

9.6.4.依赖方的陈述与担保

证书依赖方必须熟悉本 CP 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电子签名的有效性。

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 CP 的所有条款，尤其是本 CP 中关于本机构责任限制的规定，同时证书依赖方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，应当免除本机构的责任。

1、订户在申请和使用 CA 机构数字证书时，有违反如下义务之一的：

（1）订户有义务提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信息。如已提供的材料或信息有变更，可能影响证书使用的，订户应当及时通知 CA 机构。如因材料或信息变更未及时通知 CA 机构，给订户本人或第三方造成的损失，CA 机构不承担责任；

（2)订户应当妥善保管 CA 机构所签发的数字证书载体、私钥、保护密码 PIN 码，不得泄漏或随意交付他人；

（3）订户在应用自己的密钥或使用数字证书时，应当使用可依赖、安全的系统；

（4）订户知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知 CA 机构及相关各方，并终止使用该电子签名制作数据；

（5）订户在使用数字证书时必须遵守国家的法律、法规和行政规章制度，不得将数字证书用于未经授权或其他非法的目的；

（6）订户必须在证书有效期内使用该证书，不得使用已失密或可能失密已过有效期、被冻结、被撤销的数字证书；

（7）订户有义务根据规定按时向 CA 机构交纳服务费用。

2、由于下列依赖方的原因造成的损失，CA 机构不承担任何赔偿责任，由依赖方自行承担。

（1）依赖方未经检验证书的状态即决定信赖证书的；

（2）依赖方明知或者应当知道证书存在超范围使用、超期限使用、被人窃取或者信息错误等情况，仍然信赖该证书并从事有关活动的。

3、外部注册机构或其他合作方依据协议约定或实际上承担履行证书服务相关工作的，因其违反协议约定或存在过错，导致订户、依赖方或自身遭受损失的，订户或依赖方可以追究注册机构或合作方的责任，CA 机构给予配合，但 CA 机构不承担赔偿或补偿责任。

4、由于客观意外或其他不可抗力事件原因而导致数字证书签发错误、延迟中断、无法签发，或暂停、终止全部或部分证书服务的。关于不可抗力的描述参见 9.16.5。

5、因 CA 机构的设备或网络故障等技术故障而导致数字证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之“技术故障”引起原因包括但不限于：（1）不可抗力；（2）关联单位如电力、电信、通讯部门而致；（3）黑客攻击；（4）设备或网络故障。

6、如果 CA 机构能够证明其提供的服务是符合法律、行政法规相关规定实施的，CA 机构将不对订户或依赖方承担任何赔偿或补偿责任。

9.8.有限责任

1、本机构所有的赔偿义务不高于本 CP9.9 规定的赔偿责任上限。

2、本 CP 是否有相反或不同规定，就以下损失或损害，CA 机构不承担任何赔偿和/或补偿责任:

(1)订户和/或依赖方的任何间接损失、直接或间接的利润或收入损失、信誉或商誉损害、任何商机或契机损失、失去项目、以及失去或无法使用任何数据、无法使用任何设备、无法使用任何软件；

(2)由上述第(1)项所述的损失相应生成或附带引起的损失或损害；

(3)非 CA 机构的行为而导致的损失；

(4)因不可抗力而导致的损失，如罢工、战争、灾害、恶意代码病毒等。

9.9.赔偿

本机构按照本 CP9.7 和 9.8 条款具有担保免责和承担有限赔偿责任。本机构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。

本机构对于所有当事实体(包括但不限于订户、申请人或依赖方)的合计责任的赔偿金额上限为该对应数字证书服务费的十倍。这种赔偿上限可以由 CA 机构根据情况重新制定，CA 机构会将重新制定后的 CPS 公布于 CA 机构网站以通知相关当事人。如在本 CPS 公布修订的 1 个月后继续使用 CA 机构提供的数字证书服务，即表明同意接受此等修订的约束。如果不予接受本 CPS 中的约束，订户可以停止使用证书或在上述期限内以书面形式向 CA 机构申请撤销证书。

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电子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。本机构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本机构和注册机构名誉或经济损失，订户和依赖方应承担赔偿本机构和有关各方名誉或经济损失的责任。

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 本机构和注册机构名誉或经济损失，订户和依赖方应承担赔偿本机构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、未向本机构提供真实、完整和准确的信息，而导致本机构或有关各方损失。

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，未及时告知本机构，并终止使用该证书，而导致本机构或有关各方损失。

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电子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，即违反本机构对证书使用的规定，造成了本机构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

本 CP 在本机构官方网站（https://www.hbca.org.cn/）公布之日起生效，除非 本机构特别声明本 CP 提前终止。

本 CP 中将详细注明版本号及发布日期，最新版本请访问本机构官方网站（https://www.hbca.org.cn/），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 CP 正式公布生效时，旧版本的 CP 自动终止。

9.10.3.效力的终止与保留

本 CP 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

本机构及其注册机构在必要的情况下，如在主动撤销订户证书、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 CP 不适用时，由本机构安全策略委员会组织编写小组进行修订。修订完成后，本机构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 CP。

9.12.2.通知机制和期限

本 CP 在本机构的网站上发布。如在修订发布后 20 个工作日内，证书申请者和订户没有请求撤销其证书，将被视为同意该修改。

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 CP。

9.13.争议处理

本机构、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、当事人首先通知本机构，根据本 CP 中的规定，明确责任方；

2、由本机构相关部门负责与当事人协调；

3、若协调不成，当事人因与本机构或授权机构在电子认证活动中产生的任何争端及或对本 CP 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 CP 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 CP 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 CP 将替代先前的、与主题相关的书面或口头解释。

9.16.2.转让

本机构、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 CP 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 CP 无效。

9.16.4.强制执行

免除一方对 CP 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 CP 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，本机构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名方不得提出异议或申请任何补偿。

9.17.其他条款

本机构对本 CP 拥有最终解释权。