HNCA

电子认证业务规则

（版本7.1）

（生效日期：2020年9月1日）

华测电子认证有限责任公司

CTI Certificate Authority Co.,Ltd.

版权声明

地址：河南省郑州市郑东新区商务内环路26号3层；邮编：450046；电话：0371-60303977；传真：0371-60303978；电子邮件：cps@cti-cert.com。

本业务规则的最新版本请参见本公司网站https://www.hnca.com.cn，除法律法规另有要求，不再针对特定对象另行通知。

HNCA的安全策略管理委员会负责本业务规则的解释。

注意：

HNCA电子认证服务遵从中华人民共和国的法律，对于任何因违反法律行为而影响HNCA电子认证服务的个人、机构或其它组织，HNCA将保留所有的法律权利，以维护HNCA的利益。

HNCA电子认证业务规则修订表

版本	发布日期	备注
1.0	2003年6月1日	采用RFC3467结构
2.0	2006年4月15日	根据《电子认证业务规则规范（试行）》修订
3.0	2008年4月5日	根据《电子认证业务规则规范（试行）》 《中华人民共和国电子签名法》 《电子认证服务管理办法》修订
4.0	2011年6月8日	根据《电子认证业务规则规范（试行）》修订
5.0	2016年6月30日	根据《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》修订
6.0	2017年6月1日	根据公司名称变更及组织架构调整进行修订
7.0	2018年4月13日	根据新的业务模式进行修订
7.1	2020年9月1日	根据公司信息变化、业务发展进行部分细则修订。

目　录

1. 概括性描述

1.1 概述

HNCA是在国家“互联网电子身份认证示范工程”的基础上扩建而成，经原信息产业部、国家密码管理局及河南省人民政府批准，成立于2003年1月，是权威的第三方电子认证服务机构，专门负责为组织机构、个人、网站和设备等提供网上身份认证和信息安全服务。

电子认证业务规则（CPS，Certification Practice Statement）是电子认证服务机构（CA，Certificate Authority）对所提供的认证及相关业务的全面描述。

HNCA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》、《电子认证服务密码管理办法》、《电子政务电子认证服务管理办法》等电子认证服务行业的相关法律法规和管理规定，遵循《电子认证业务规则规范》的要求，制定了《HNCA电子认证业务规则》，并报工业和信息化部备案。

本CPS适用于HNCA及其员工、注册机构、订户、依赖方、合作方和其他参与者。各参与方必须完整地理解和执行本CPS所规定的条款，并承担相应的责任和义务。

1.2 文档名称与标识

本文档名称是《HNCA电子认证业务规则》，简称《HNCA-CPS》。

1.3 电子认证活动参与方及其职责

1.3.1 电子认证服务机构

HNCA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》、《电子认证服务密码管理办法》和《电子政务电子认证服务管理办法》等规定，依法设立的权威第三方电子认证服务机构，是对证书的签发、发布、更新、撤销等证书全生命周期进行管理的实体。

1.3.2 注册机构

注册机构（RA）作为电子认证服务机构授权委托的实体，可分为本地注册机构和远程注册机构，负责受理证书的申请、审核、更新、恢复、撤销和下载等业务。

HNCA本身是CA，也承担RA职责，还可以授权建立外部RA，并管理合作方。

RA有责任妥善保存客户的数据，不允许将客户的数据透露给与证书申请无关的任何单位或个人，不允许用作商业利益方面的用途。RA对其提供的证书服务负有相关的法律责任，包括但不限于本CPS和授权协议中所规定的有关内容。

1.3.3 订户

订户是从电子认证服务机构接收证书的实体。在电子签名应用中，订户即为电子签名人。

在HNCA电子认证服务体系中，订户包括组织机构(包括但并不限于党政机关、企事业单位、社会团体等）、个人、服务器、网站等各类具有确定身份标识的主体或实体。

1.3.4 依赖方

依赖方是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。在HNCA证书服务体系中，依赖方是指依赖HNCA订户证书及其数字签名进行决策和业务活动的实体。

非HNCA订户的依赖方，HNCA除了担保其所信任的并且由HNCA签发的证书和相关签名信息的真实性以外，不承担其它义务和责任。

1.3.5 合作方

特定情况下，HNCA同合作方建立合作关系，以便能够向订户和依赖方提供更为优质和全面的服务。在约定的合作框架内，HNCA将订户数字证书生命周期内的全部或部分管理工作，由合作方进行办理，且规定该订户证书仅在HNCA同合作方

约定的业务范围内适用。数字证书生命周期的管理内容包括但不限于证书的申请、审核、更新、撤销以及交付等。

合作方应明确自身证书管理工作的内容、边界以及安全风险，同时承担相关的法律责任和义务，包括但不限于本CPS和授权协议中所规定的有关内容。

1.3.6 其他参与者

其他参与者指为 HNCA 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

证书类型及用途参见 HNCA 网站 https://www.hnca.com.cn 上的介绍，订户和依赖方等主体应依据自身需要决定使用的证书类型。

1.4.2 限制的证书应用

各类证书的使用应符合证书内容对其用途的限定，如参与方未经HNCA认可或不遵守相关约定，其对证书的应用超出限定的应用范围，将不受HNCA的保护。

HNCA签发的证书禁止在违反国家法律、法规或破坏国家安全的情况下使用，由此造成的法律后果由订户负责。

1.5 策略管理

1.5.1 策略文档管理机构

本CPS的管理机构是HNCA的安全策略管理委员会。安全策略管理委员会下设执行组，执行组主要成员由各相关部门人员组成。执行组负责编写、修订CPS。

1.5.2 联系人

本CPS在HNCA网站发布，对具体个人不另行通知。

网站地址：https://www.hnca.com.cn；

电子邮箱地址：cps@cti-cert.com；

联系地址：河南省郑州市郑东新区商务内环路26号3层；

邮政编码：450046；

电话号码：0371-60303977；

传真号码：0371-60303978。

1.5.3 决定 CPS 符合策略的机构

HNCA的安全策略管理委员会负责本CPS的制订、发布、更新以及此方面的对外咨询服务等事宜。

1.5.4 CPS 批准程序

安全策略管理委员会执行组（以下简称“执行组”）负责起草CPS形成讨论稿，并征求公司领导和各部门意见，达成一致意见后提交安全策略管理委员会审阅；执行组依据安全策略管理委员会评审意见完成修改后提交公司行政部门；公司行政部门确定CPS文本格式和版本号，形成定稿，报安全策略管理委员会主任审批；安全策略管理委员会主任审批同意后，方可对外发布。

公司行政部门负责自发布之日起30天内向工业和信息化部备案。

1.6 定义和缩写

下列定义适用于本CPS：

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

PKI利用公钥密码理论和技术实施和提供信息安全服务的普适性安全基础设施，是硬件、软件、人员、策略和操作规程的总和，完成证书的发放、管理和使用，并基于证书提供信息安全服务。

b) 电子认证业务规则（CPS）Certification Practice Statement

电子认证业务规则是电子认证服务机构对所提供的认证及相关业务的全面描述。

c) 电子认证服务机构（CA）Certification Authority

对证书的签发、发布、更新、撤销等证书全生命周期进行管理的权威第三方机构。

d) 注册机构（RA）Registration Authority

具有下列一项或多项功能的实体：识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动撤销证书，处理订户撤销其证书的请求，同意或拒绝订户更新其证书或密钥的请求。但是，RA 并不签发证书（即 RA 代表 CA 承担某些任务）。

e) 电子签名认证证书(证书)Digital Certificate

由电子认证服务机构（CA）签名的包含公钥拥有者信息、公钥、签发者信息、有效期以及扩展信息的一种电子文件。

f) 证书撤销列表 (CRL)Certificate Revocation List

由电子认证服务机构（CA）签发并发布的被撤销证书的列表，也称黑名单服务。

g) 注销列表（ARL）Certificate Authority Revocation List

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

h) 私钥(电子签名制作数据) Private Key

非对称密码算法中指只能由拥有者使用的不公开密钥。签名者使用私钥对待签名数据做数字签名，得到签名值。

i) 公钥(电子签名验证数据) Public Key

非对称密码算法中可以公开的密钥。验证者使用签名者的公开密钥对签名值进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

2. 信息发布与信息管理

2.1 认证信息的发布

HNCA信息库面向认证服务各参与方提供信息服务，包括但不限于以下内容：证书、CRL、CPS、证书服务协议、技术支持手册和HNCA不定期发布的信息。

HNCA信息库不会改变任何从电子认证服务机构发出的证书和任何证书撤销的通知，而是准确描述上述内容。处理任何与HNCA相关的事宜时，必须使用HNCA

信息库作为主要的和正式的依据。

HNCA通过网站公布以下信息：本CPS修订以及其他由HNCA不定时发出的信息。HNCA网址：https://www.hnca.com.cn。

HNCA通过目录服务器发布订户的证书和CRL，各参与方可以通过访问HNCA的目录服务器获取证书的信息和撤销证书列表。同时，HNCA提供在线证书状态查询服务。

2.2 发布时间或频率

HNCA应在https://www.hnca.com.cn上及时发布CPS的最新版本；

HNCA签发的证书在订户收到证书后应实时发布；

HNCA的CRL最迟24小时发布一次；

HNCA应在https://www.hnca.com.cn上实时发布其他与电子认证服务相关的公告和通知。

2.3 信息库访问控制

对于公开发布的信息，HNCA允许各参与方通过网站或目录服务器进行查询和访问。

HNCA的安全访问控制机制确保只有经过授权的人员才能编写和修改信息库中的信息，但不限制对这些信息的阅读权。

3. 身份标识与鉴别

3.1 命名

3.1.1 名称类型

HNCA采用X.500定义的唯一甄别名DN（Distinguished Name）来标识订户身份信息，该甄别名包含于证书主体中。

3.1.2 对名称意义化的要求

订户的甄别名(DN)必须具有一定的意义，能够与证书主体所对应的实体建立确定联系。

3.1.3 订户的匿名或伪名

在HNCA证书服务体系中，订户不允许使用匿名或伪名申请证书。

3.1.4 理解不同名称形式的规则

HNCA所签发证书的甄别名DN符合X.500命名规则，命名规则如下：

编号	识别名称	说明	内容（示范性）
1	County（C）	国家名称	C=CN
2	Organization(O)	组织机构名称	O=HNCA
3	Organization Unit（OU）	部门名称	OU=技术中心
4	Common Name（CN）	订户的一般通用名称	CN=李白
5	Location（L）	所在城市	L=郑州
6	State（ST）	所在省	ST=河南

如果有C项，则放在最后，且C=CN；

如果有CN项，则放在DN的最前面；

如果同时存在OU和O项，则OU在O前面；如果同时存在ST和L项，则L在ST前面。

3.1.5 名称的唯一性

在HNCA证书服务体系中，订户的主体名称必须是唯一的。

3.1.6 商标的承认、鉴别和角色

3.2 初始身份确认

3.2.1 证明持有私钥的方法

HNCA通过包含数字签名的证书请求数据（如PKCS#10）来证明订户持有私钥。HNCA的电子认证服务系统使用订户的公钥验证由订户私钥签名的证书请求数据，来证明证书申请人持有与证书申请数据中公钥相对应的私钥。

3.2.2 组织身份的鉴别

对于组织身份的鉴别，需要查验组织的合法证照。

申请者须持包括但不限于工商营业执照等证照，以及组织给经办人的授权证明和经办人身份证件，向HNCA或其授权的RA和合作方提出申请。如该组织需申请含域名、IP地址和邮件地址的证书，还需提交相关证明其拥有此项权利的资料。

如果HNCA或其授权的RA和合作方可以通过第三方验证或其他非现场方式明确组织身份时，接受申请者通过传真、邮递、网络以及HNCA认可的其他方式递交申请材料。

申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。

HNCA或其授权的RA和合作方可以通过查询第三方数据库、访问政府相关信息公示平台、咨询相应机构及其他合法途径，对申请者提交的申请材料进行查验。

HNCA或其授权的RA和合作方应妥善保存申请者的申请材料。

特定情况下，合作方进行组织身份鉴别时，其身份鉴别过程由 HNCA 和合作方的合作协议约定。

3.2.3 个人身份的鉴别

申请者应提交个人身份证明材料，HNCA支持的有效证件类型包括身份证、户口本、护照及其电子副本等合法有效证件。

如果HNCA或其授权的RA和合作方可以通过第三方验证或其他非现场方式明确个人身份时，接受申请者可以通过传真、邮递、网络以及HNCA或合作方认可的其他方式递交申请材料。

申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。

HNCA或其授权的RA和合作方可以通过查询第三方数据库、访问政府相关信息公示平台、咨询相应机构及其他合法途径，对申请者提交的申请材料进行查验。

HNCA或其授权的RA和合作方应妥善保存申请者的申请材料。

特定情况下，合作方进行个人身份鉴别时，其身份鉴别过程由 HNCA 和合作方的合作协议约定。

3.2.4 可信组织个人身份的鉴别

HNCA可基于对组织身份的鉴别，认为该组织为可信组织，可授权该组织对HNCA认可范围内的员工进行内部身份鉴别，需要：

1）通过可靠的方式确保证书持有者所在的组织、部门与证书中所列的组织、部门一致，证书中通用名就是证书持有者的真实姓名；

2）确认证书持有者属于该组织机构，证书持有者确实被招录或聘用。。

被授权的组织有义务在HNCA需要时提供证书持有者的身份鉴别材料，并对其真实性负责。

3.2.5 没有验证的订户信息

除该类型证书所必须要求的身份信息需要得到明确、可靠的验证以外，HNCA不对申请时的其他信息予以验证。

对于没有验证过的订户信息，HNCA将不承诺此类信息的真实性，并不承担由于此类信息引起的任何责任和解决纠纷的义务。

3.2.6 授权确认

在个人或者组织机构委托经办人申请证书时，HNCA或其授权的RA和合作方需审核经办人的身份和资格，包括必需的身份证明材料和授权证明(按要求填写的《HNCA企业（个人）数字证书业务受理单》含授权证明)，对授权予以确认。

特定情况下，合作方代表个人或组织机构申请证书时，HNCA 对合作方提出的申请视为个人或组织机构对合作方的授权确认。

3.2.7 互操作准则

互操作可能是交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各自认证策略的CA之间建立相互信任关系，从而使双方的订户可以实现互相认证。

HNCA将根据业务需要，在遵循本CPS的各项控制要求的基础上，与HNCA证书服务体系中未涉及的其他电子认证服务机构建立交叉认证关系。但交叉认证并不表示HNCA批准了或赋予了其他CA或电子认证服务机构的权力。

3.3 密钥更新请求的身份标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

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，HNCA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 撤销后密钥更新的标识与鉴别

撤销后密钥更新时，对订户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。

3.4 撤销请求的标识与鉴别

订户本人撤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，由注册机构申请撤销订户的证书时，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

证书申请实体包括组织机构(包括但并不限于党政机关、企事业单位、社会团体等）、个人、服务器、网站等各类具有确定身份标识的主体或实体。

4.1.2 申请过程与责任

证书申请人按照本CPS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。HNCA或其授权的RA和合作方依据§3.2.2组织身份的鉴别和§3.2.3个人身份的鉴别，对证书申请人的身份进行鉴别，并决定是否受理申请。

证书申请实体要按照本CPS的要求准备证书申请材料，并确保申请材料真实准确。

HNCA或其授权的RA和合作方负责接收证书申请实体的请求材料，对所提供的申请信息与身份证明资料的一致性进行查验，对证书申请进行批准或拒绝。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

HNCA或其授权的RA和合作方按照本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

HNCA或授权的RA和合作方根据本CPS所规定的身份鉴别流程对证书申请人身份进行识别与鉴别后，根据鉴别结果决定批准或拒绝证书申请。

如果证书申请人通过本CPS所规定的身份鉴别流程且鉴证结果为合格，HNCA

或授权的RA和合作方将批准证书申请，为证书申请人制作并颁发证书。

证书申请人未能通过身份鉴证，HNCA或授权的RA和合作方将拒绝申请人的证书申请，并通知申请人鉴证失败，同时向申请人提供失败的原因（法律禁止的除外）。

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

4.2.3 处理证书申请的时间

HNCA或其授权的RA和合作方确认证书申请信息，一旦注册机构收到了所有必须的相关信息，将在1～3个工作日内处理证书申请。

HNCA或其授权的RA和合作方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HNCA的管理要求。

4.3 证书签发

4.3.1 证书签发过程中电子认证服务机构的行为

HNCA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最终完全正式地批准了证书申请。

通常，HNCA所签发的证书在24小时内生效。

4.3.2 电子认证服务机构对订户的通告

HNCA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HNCA或其授权的RA和合作方领取证书；

b) 通过电子邮件（e-mail）方式或短信通知；

c) 邮政信函通知；

d) 其他HNCA或其合作方认为安全可行的方式。

HNCA没有上门为订户安装证书的义务。如果订户需要，HNCA可以上门安装，但需要收取相应的服务费用。HNCA或其授权的RA和合作方提供热线支持服务。热线支持电话由HNCA或其授权的RA和合作方公布。

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，HNCA或其授权的RA和合作方将证书本身或者证书获得的方式或者与证书相关的授权码递送给证书申请人，即视为证书申请人同意接受证书。

4.4.2 电子认证服务机构对证书的发布

HNCA在签发完证书后，将证书发布到数据库和目录服务器中。

HNCA采用主、从目录服务器结构来分布所签发证书。签发完成的数据直接写入主目录服务器中，然后通过主从映射，将主目录服务器的数据自动发布到从目录服务器中，供订户和依赖方查询和下载。

4.4.3 电子认证服务机构在颁发证书时对其他实体的通告

其他实体可以通过从目录服务器中查询到 HNCA 已经签发的证书。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户在提交了证书申请并接受了HNCA所签发的证书后，均被视为已经同意遵守与HNCA、依赖方有关的权利和义务的条款。订户接受了证书，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，并按照证书内容对证书用途的约束（如密钥用途、密钥扩展用途）使用私钥和证书。并且在证书到期或被撤销之后，订户必须停止使用该证书对应的私钥。

4.5.2 依赖方对公钥和证书的使用

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）。依赖方获得对方的证书和公钥后，可以通过查看对方的证书了

解对方的身份，并通过公钥验证对方电子签名的真实性和验证证书的有效性。在验证电子签名时，依赖方应准确知道签名的数据格式和信息范围，能确定什么数据已被签名。

验证证书的有效性包括三个方面的内容：

a）用HNCA的证书验证证书中的签名，确认该证书是HNCA签发的，并且证书的内容没有被篡改；

b）检验证书的有效期，确认该证书在有效期之内；

c）查询证书状态，确认该证书没有被撤销。

4.6 证书更新

证书更新是指在不改变证书中订户的公钥或其他任何信息的情况下，为订户签发一张新证书。出于安全原因，除非订户提出特别申请并确保原证书密钥对的安全，HNCA将使用证书密钥更新过程来处理订户的证书更新请求。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

a）证书的有效期将要到期；

b）因私钥泄漏而撤销证书；

c）证书无法继续获得信任；

d）证书无法正常使用；

e）证书丢失；

f）订户自主提出更新；

g）HNCA因法律法规、行业政策或自身策略要求更新。

4.7.2 请求证书密钥更新的实体

持有HNCA证书的订户，包括组织机构(包括但并不限于党政机关、企事业单位、社会团体等）、个人、服务器、网站等各类具有确定身份标识的主体或实体，都可以请求证书密钥更新。

4.7.3 证书密钥更新请求的处理

处理证书密钥更新请求可以采用两种方式：

一种方式是在线更新。对于证书信息无须改变的订户，申请更新的实体在线向HNCA提交更新申请，HNCA验证申请更新者拥有与证书对应的私钥后，为其签发新的证书。

另一种方式是人工方式更新。由HNCA或其授权的RA和合作方来处理证书更新请求，为订户制作新的证书。订户注册信息没有发生变化的，HNCA或其授权的RA和合作方可以依据原注册信息对其签发新的证书。

4.7.4 颁发新证书对订户的通告

在线更新方式，给订户颁发新证书时，在线更新系统会自动通知证书更新已完成。

人工更新方式，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HNCA或其授权的RA和合作方领取证书；

b) 通过电子邮件（e-mail）方式或短信通知；

c) 邮政信函通知；

d) 其他HNCA或合作方认为安全可行的方式。

4.7.5 构成接受密钥更新证书的行为

同§4.4.1构成接受证书的行为。

4.7.6 电子认证服务机构对密钥更新证书的发布

同§4.4.2电子认证服务机构对证书的发布。

4.7.7 电子认证服务机构在颁发证书时对其他实体的通告

同§4.4.3电子认证服务机构在颁发证书时对其他实体的通告。

4.8 证书变更

4.8.1 证书变更的情形

证书变更是指证书申请订户关键信息有变更，导致证书内容有变化，需要重新制作证书的情形。

4.8.2 请求证书变更的实体

持有HNCA证书的订户，包括组织机构(包括但并不限于党政机关、企事业单位、社会团体等）、个人、服务器、网站等各类具有确定身份标识的主体或实体，都可以请求证书变更。

4.8.3 证书变更请求的处理

HNCA将使用证书密钥更新过程来处理订户的证书变更请求。

4.9 证书撤销和挂起

4.9.1 证书撤销的情形

a) 发生下列情形之一的，订户应当申请撤销证书：

- 证书私钥泄露；
- 证书中的信息发生重大变更；
- 认为本主体或实体不能实际履行HNCA-CPS。

b) 发生下列情形之一的，HNCA可以撤销其签发的证书：

- 订户申请撤销证书；
- 订户提供的信息不真实；
- 订户没有履行双方合同规定的义务；
- 证书的安全性得不到保证；
- 法律法规和行业政策规定的其他情形。

4.9.2 请求证书撤销的实体

根据不同的情况，订户、HNCA或其授权的RA、合作方、司法机关及其他公权力机关可以请求撤销订户证书。

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:

a) 证书撤销的申请人到HNCA或其授权的RA和合作方按要求填写《HNCA企业(个人)数字证书业务受理单》勾选“撤销”选项;

b) HNCA或其授权的RA和合作方对订户提交的撤销请求进行审核，详见§3.2.2组织身份的鉴别和§3.2.3个人身份的鉴别。

c) HNCA撤销订户证书后，HNCA或其授权的RA和合作方将通知订户证书被撤销。

d) 强制撤销是指当HNCA或其授权的RA和合作方确认订户有违反本CPS的情况发生时，对订户证书进行强制撤销，撤销后将立即通知该订户。

e）证书撤销信息在24小时内发布。

4.9.4 撤销请求宽限期

如果出现私钥泄露等事件，订户必须在发现泄露或有泄露嫌疑8小时内提出撤销请求。其他原因引起的撤销请求订户必须在48小时内提出。

4.9.5 电子认证服务机构处理撤销请求的时限

证书撤销的申请人到HNCA或其授权的RA和合作方按要求填写《HNCA企业(个人)数字证书业务受理单》，HNCA在对撤销请求审核通过后实时处理。HNCA24小时内将最新的CRL发布到目录服务器指定的位置，供订户和依赖方查询下载。

4.9.6 依赖方检查证书撤销的要求

在具体应用中，依赖方必须使用以下两种功能之一进行所依赖证书的状态查询：

a) CRL查询：利用证书中标识的CRL地址，通过目录服务器提供的查询系统，查询并下载CRL到本地，进行证书状态的检验。

b)在线证书状态查询：服务系统接受证书状态查询请求，证书状态查询结果经过签名后，返回给请求者。

依赖方应验证CRL的可靠性和完整性，确保是经HNCA发布并且签名的。

4.9.7 CRL 的颁发频率

HNCA可采用实时或定期的方式发布CRL。HNCA一般每4小时签发一次CRL。

4.9.8 CRL 发布的最长滞后时间

发布的最长滞后时间为24小时。

4.9.9 证书挂起

HNCA暂不提供证书挂起服务。

4.10 证书状态服务

4.10.1 操作特点

HNCA通过目录服务器和证书在线状态查询服务系统为各参与方提供证书状态查询服务。

4.10.2 服务可用性

HNCA提供7X24小时的证书状态查询服务。即在网络允许的情况下，各参与方能够实时获得证书状态查询服务。

4.11 订购结束

订购结束是指当证书有效期满或证书撤销后，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，视

为订购结束；

b）在证书有效期内，证书被撤销后，即订购结束。

4.12 密钥生成、备份与恢复

4.12.1 密钥的生成和备份

HNCA颁发的订户证书中，含有签名用途的密钥对由订户自己生成。

订户的加密密钥对由河南省密钥管理中心（KMC）生成和备份。

4.12.2 密钥的恢复

密钥恢复是指加密密钥的恢复，密钥管理基础设施不负责签名密钥的恢复。密钥恢复分为以下两类：

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还原，此时订户可申请密钥恢复。订户向HNCA或其授权的注册机构申请，经身份证明材料鉴别验证审核后，通过HNCA向密钥管理基础设施请求；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：司法取证人员向HNCA提交申请，经审核后，通过密钥管理基础设施的密钥恢复模块恢复所需的密钥，并记录于特定载体中。

5. 电子认证服务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

HNCA电子认证服务系统的机房位于河南省郑州市郑东新区商务内环路26号3层。场地具有三道物理防护，以监控和管理HNCA机房的物理通道。河南地处中原，发生地震等自然灾害的概率较小，机房具备独立的防震、防火、防水、温控、门禁系统、视频监控系统和警报系统等，可以保证认证服务的连续性和可靠性。

机房内部禁止参观、拍照、摄像。机房采用高安全性的监控技术，包括视频、指纹、门禁等安全管理手段，以确保物理通道的安全。进入HNCA机房时，有延时报警门禁系统。机房实行全天候自动监控。监控记录文件包括对机房通道上的所有踪迹的记录。所有进入HNCA机房的来访者只有经过批准后，经由HNCA人员陪同，才能在限制区域内活动。

HNCA的建筑物和机房建设按照下列标准实施：

a) GB 50174-93：《电子计算机机房设计规范》；

b) GB 2887-89：《计算站场地技术条件》；

c) GB 9361-88：《计算站场地安全要求》；

d) GB 6650-1986：《计算机机房用活动地板技术条件》；

e) GB 50034-1992：《工业企业照明设计标准》；

f) GB 5054-95：《低压配电装置及线路设计规范》；

g) GHN 19-87：《采暖通风与空气调节设计规范》；

h) GB 157：《建筑防雷设计规范》；

i) GHN 79-85：《工业企业通信接地设计规范》。

5.1.2 物理访问

为保证本系统的安全，采取了一定的隔离、控制、监控手段。机房通过设置门禁和侵入报警系统来保护机房物理安全。

物理访问控制包括如下几个方面：

a) 门禁系统：工作人员需使用密码结合指纹鉴定才能进出，系统保留时间记录和信息提示。

b) 报警系统：当发生任何非法闯入、非正常手段开门、长时间不关门等异常情况都会触发报警系统。

c) 监控系统：对HNCA机房进行24小时不间断录像，系统保留录像资料，以备查询。

5.1.3 电力与空调

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统，

按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备分开供电。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。

机房使用不间断电源（UPS）来保证供电的稳定性和可靠性。机房采用双电源接入，在单路电源损坏时，可以自动切换，维持系统正常运转。

根据机房环境及设计规范要求，均设置了空气调节系统。空调系统由精密空调、通风管路、新风系统组成。

HNCA参照电信设施管理的规定进行维护和保养。

5.1.4 水患防治

HNCA机房位于建筑物中间层，机房内无上下水系统，空调间做了严格防水处理，发生水患的可能性很小。

HNCA机房内无渗水、漏水现象，主要设备采用专用的防水插座，并采取必要措施防止下雨或水管破损，造成天花板漏水、地板渗水和空调漏水等现象。

5.1.5 火灾预防和保护

机房所在建筑物的耐火等级符合GHN45《高层民用建筑设计防火规范》中规定的二级耐火等级，通过了国家权威部门的消防测试。HNCA设施内设置火灾报警装置。在机房内、各物理区域内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位设置烟、温感探测器。机房采用防火材料建设，配置独立的气体灭火装置，使用专业的灭火系统，备有相应的气体灭火器，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂。工作区配置水喷淋灭火装置。HNCA通过与专业防火部门协调，建立了消防灭火等应急响应措施。

5.1.6 介质存储

数据的存储介质包括硬盘、光盘等，介质存储地点保证物理安全，能够防磁、防静电干扰、防火、防水，由专人管理。

5.1.7 废物处理

当HNCA存档的敏感数据或密钥已不再需要或存档期限已满时，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

HNCA定期进行数据备份，备份数据保存于指定的银行保险箱。

5.2 程序控制

5.2.1 可信角色

电子认证服务各参与方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：

a) 系统管理员

系统管理员负责对证书服务体系在本单位的系统进行日常管理，包括应用系统及其操作系统，执行系统的日常监控，并可根据需要签发服务器证书和下级操作员证书。

b) 安全管理员（安全经理）

安全管理员（安全经理）对HNCA的物理、网络、系统的安全全面负责。并且拟订安全管理制度和操作流程，监督各岗位安全管理的执行情况。

c) 审计员

审计员控制、管理、使用审计系统，审计系统分布于管理系统的各个子系统中，负责各个子系统的运行和操作日志记录。

d) 密钥管理员

密钥管理员负责管理数字认证中心的密钥相关设备，进行CA中心密钥的生成、备份、恢复、销毁等操作。

e) 业务管理员

业务管理员对注册机构操作员进行管理，并对注册机构业务进行管理。

f) 业务操作员

业务操作员进行录入、审核、制作等证书业务操作，直接对订户提供服务。

g) 客户服务人员

客户服务人员向客户提供关于证书申请及使用方面的问题，直接对订户服务。

5.2.2 每项任务需要的人数

HNCA制定了规范的策略，严格控制任务和职责的分割，基于工作要求和工作安排建立任务和职责分割制度，贯彻互相牵制、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。

a) 访问和管理CA的加密设备及密钥，至少需要3个可信人员。

b) 对于证书的申请鉴别和签发，需要2个可信人员操作完成。

c) 对于重要的系统数据操作和重要系统维护，需要安排至少1人进行操作，1人进行监督记录。

5.2.3 每个角色的识别与鉴别

HNCA在聘用可信角色人员之前，均会按照本CPS §5.3.2背景审查程序的规定对其进行背景审查。所有HNCA的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用密码结合指纹识别；进入系统需要使用证书进行身份鉴别。HNCA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

需要进行职责分割的角色，包括但不限于下列人员：

a) 从事证书申请信息验证的人员；

b) 负责证书申请、撤销、更新和信息注册等服务请求的批准、拒绝或其他操作的人员；

c) 负责系统管理的人员；

d) 负责网络管理的人员；

e) 负责数据管理的人员；

f) 负责密钥及密码设备管理、操作人员。

对于证书服务的受理，应通过录入员、审核员2个角色才能完成。

对于CA密钥的操作，必须有3名以上的CA密钥管理员同时到场，才能进行有关操作。

5.3 人员控制

5.3.1 资格、经历和无过失要求

所有的员工与HNCA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，具体要求在人事管理制度中规定。HNCA要求充当可信角色的人员至少必须具备忠诚、可信赖及工作的热诚度、无影响CA运行的其他兼职工作、无同行业重大错误记录、无违法记录等。

5.3.2 背景审查程序

背景调查分为：基本调查和全面调查。

基本调查包括对工作经历、职业推荐、教育、社会关系方面的调查。

全面调查除包含基本调查项目外还包括对是否有无犯罪记录等调查。

调查程序包括：

a) 用人部门通过面对面沟通互动、情景模拟等方式对其考察。

b) 人事部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。

c) 人事部门通过电话、信函、网络、走访等形式对其提供的材料的真实性进行核查。

d) 核查合格后，经主管领导批准后准予上岗。

必要时，HNCA可以与有关的政府部门和调查机构合作，对指定的可信人员进行背景调查。

5.3.3 培训要求

HNCA对员工的一般培训内容为：证书基础知识、电子认证相关法律法规、HNCA-CPS、规章制度、企业文化、岗位职责等。

针对特殊岗位员工，培训内容包括但不限于以下内容：HNCA电子认证服务系统、身份验证和审核策略和程序、灾难恢复和义务连续性程序、电子认证服务项目管理、电子认证相关产品体系等。

5.3.4 再培训周期和要求

HNCA策略调整、系统更新时，应组织员工进行继续培训，以适应新的变化。

对于公司安全管理策略，每年至少进行1次培训；认证系统运营相关的人员，每年至少进行1次相关技能和知识培训。

HNCA根据实际情况，对PKI/CA和密码技术的发展和演变，安排相应的培训。

HNCA每年选派人员，参与行业组织的专项培训。

5.3.5 工作轮换周期和顺序

对于可替换角色,HNCA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 对未授权行为的处罚

当HNCA员工被怀疑，或者已进行了未授权的操作，例如滥用权利或超出权限使用HNCA系统或进行越权操作，HNCA得知后将立即对该员工进行工作隔离，并对该员工的未授权行为进行评估，根据评估结果按照公司规定进行相应处罚。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

HNCA因特殊需要聘请第三方人员参与指定工作时，必须对其进行必要的知识培训和安全规范培训，就工作内容签署保密协议，并对其从事的工作进行有效监督。

5.3.8 提供给员工的文档

为保障认证系统的正常安全运行，HNCA应该给相关员工提供有关的文档，至少包括HNCA-CPS、公司规章制度、岗位说明、相关培训资料以及与岗位相关的文档资料等。

5.4 审计日志程序

5.4.1 记录事件的类型

HNCA记录与系统相关的事件，这些记录信息称为日志。对于这些日志，无论其载体是纸张还是电子文档的形式，必须包含事件发生的日期、事件的发生时间段、事件的内容和事件相关的实体等。

HNCA还可能记录与系统不直接相关的事件，例如：物理通道参观记录、人事变动等。

5.4.2 处理或归档日志的周期

HNCA不定期对日志记录进行审查，对审查记录行为备案，每年进行的审查不少于2次。

5.4.3 审计日志的保存期限

审计日志的保存期限不低于5年。

5.4.4 审计日志的保护

HNCA执行严格的管理，确保只有HNCA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。

HNCA对审计日志备份后，存放于指定的银行保险柜。

5.4.5 审计日志备份程序

HNCA保证所有的审计日志都按照HNCA备份标准和程序进行备份。根据记录的性质和要求，分为实时、按天、按周、按月和按年等多种形式的备份，可采用在线和离线两种方式的备份工具。

5.4.6 审计日志收集系统

审计日志收集系统涉及：

a) 证书签发系统；

b) 证书注册系统；

c) 证书受理系统；

d) 证书目录系统；

e) 访问控制系统；

f) 网站、数据库安全管理系统；

g) 其他需要审计的系统。

HNCA使用系统审计工具进行对上述系统的审计日志收集。

5.4.7 对导致事件实体的通告

HNCA发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，HNCA保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

HNCA有权决定是否对导致事件的实体进行通告。

5.4.8 脆弱性评估

HNCA不定期对系统进行脆弱性评估，每年不低于1次，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

归档记录包括所有审计数据、证书申请信息、与证书申请相关的信息和证书信息等。

5.5.2 归档记录的保存期限

除了法律法规和管理部门提出的保存期限外，HNCA对与证书相关的归档记录至少保存到证书有效期结束后5年。与法律政策的规定不一致时，选择两者中较长的期限予以保存。

此外，在不违反法律法规和管理部门的规定的前提下，HNCA可以自主决定信息的存档期限，并不对此做出说明和解释。

5.5.3 归档文件的保护

存档内容采用物理安全措施或密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能查询。HNCA保护相关的档案内容，免遭恶劣环境的威胁，如温度、湿度和强磁力等的破坏。

HNCA保存的申请者和订户基本情况资料和身份鉴别资料，非经政府主管机构或者司法机构经过合法的途径予以申请，任意无关的第三方均无法获知。

5.5.4 归档文件的备份程序

所有存档的文件和数据库除了保存在HNCA指定的存储库，还可以在异地保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有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。HNCA在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

5.5.5 记录时间戳要求

所有记录都要在存档时加具体准确的时间标识以表明存档时间，可以是系统

自动标识的时间，也可以是操作员手工标注的时间，HNCA不采用时间戳技术表明存档时间。

5.5.6 归档收集系统

HNCA电子认证服务系统的相关运营信息，由内部工作人员或具备安全控制措施的内部系统，依照人工和自动操作两部分进行产生和收集，并由专人进行管理和分类。

5.5.7 获得和检验归档信息的程序

只有被授权的可信人员能够访问归档记录。归档记录的一致性在归档时进行验证。归档期间，所有被访问的记录在归还时必须验证其一致性。

5.6 电子认证服务机构密钥更替

HNCA在CA根证书到期时，需要更换密钥，具体措施如下：

由国家根CA签发的CA根证书到期前，HNCA将向国家根CA机构申请新CA根证书；新CA根证书启用时同时停止旧CA根证书的签发证书服务，过渡期内旧CA根证书的CRL签发服务继续有效，直到依赖旧CA根证书签发的证书到期为止；HNCA采取必要措施保障新旧CA根证书之间的信任过渡。

5.7 损害和灾难恢复

5.7.1 事故和损害处理程序

发生故障时，HNCA将按照灾难恢复计划实施恢复。

5.7.2 计算资源、软件和/或数据被破坏

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

5.7.3 实体私钥损害处理程序

当HNCA证实CA私钥泄露后，HNCA应:

a）向管理部门汇报，并启动电子认证服务机构密钥更替流程；

b）立即停止使用该私钥签发证书，并撤销该私钥颁发的所有订户证书；

c）通过网站、客户端、短信、电话通知和邮件等方式，告知证书订户和依赖方；

d）机构密钥更替完成后，为受影响的订户重新签发证书。

5.7.4 灾难后的业务连续性能力

HNCA的核心证书业务系统均采用双机热备方式，数据库采用磁盘阵列方式来确保证书服务的高可靠性和可用性。

HNCA有异地数据备份，发生自然灾害或其它不可抗力性灾难后，HNCA将利用备份数据重建系统恢复业务。

5.8 电子认证服务机构或注册机构的终止

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

HNCA在终止服务九十日前，就业务承接及其他有关事项通知有关各方，包括但不限于HNCA授权的RA和合作方和订户、依赖方等。

在终止服务六十日前向管理部门报告，按照相关法律规定的步骤进行操作。并与其他电子认证服务机构就业务承接进行协商，做出妥善安排。若HNCA未能就业务承接事项与其他电子认证服务机构达成协议，将向管理部门申请安排其他电子认证服务机构承接相关业务。

同时，HNCA采取以下措施终止业务：

a）起草HNCA终止业务声明；

b）停止认证中心所有业务；

c）处理加密密钥；

d）处理和存档敏感文件；

e）清除主机硬件；

f）通知与HNCA终止运营相关的实体；

g）根据运营协议终止RA和合作方的业务。

6. 认证系统技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

a）CA密钥对生成

HNCA的CA密钥对在国家密码主管部门批准和许可的硬件密码设备中生成并存放在该密码设备中，采用（3，5）秘密共享机制将密钥份额分享给5个密钥管理员保管。CA密钥对生成时，必须5个密钥管理员在场，分别将密钥份额存放在自己保管的密码设备中。

b）订户密钥对生成

订户签名密钥对由订户自主生成，加密密钥对由河南省密钥管理中心（KMC）生成。

6.1.2 私钥传送给订户

订户的签名密钥对由订户自己生成并保管。

加密密钥对由河南省密钥管理中心（KMC）产生，通过安全通道传送给订户。

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RA传送到HNCA。

订户的加密证书公钥，由KMC通过安全通道传送给HNCA。

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，保证传输中的数据安全。

6.1.4 电子认证服务机构公钥传送给依赖方

依赖方可以从HNCA网站https://www.hnca.com.cn下载根证书和CA证书，从而得到CA的公钥。

6.1.5 密钥的长度

HNCA的电子认证服务系统支持签发SM2算法证书和RSA算法证书，SM2证书密钥长度为256比特，RSA证书密钥长度为1024比特或2048比特。HNCA根据订户需求为订户签发不同算法类型和密钥长度的证书。

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局批准和许可的硬件密码设备产生。

6.1.7 密钥使用目的

a) CA密钥

CA密钥用于签发证书和CRL。

b) 订户密钥

订户密钥的用途通过订户证书中的密钥用途扩展项约定。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块标准和控制

HNCA电子认证服务系统所用的密码设备是经国家密码管理部门许可和批准的产品。HNCA所采用密码模块符合国家密码行业相关技术标准。

6.2.2 私钥的多人控制

CA私钥的生成、更新、撤销、备份和恢复等操作采用多人控制机制，将私钥的管理权限分散到5张管理员卡中，只有其中3至5人在场并许可的情况下，才能对私钥进行操作。

6.2.3 私钥托管

HNCA不向订户提供私钥托管服务。

订户加密密钥对由河南省密钥管理中心（KMC）托管，其生命周期管理由河南省密钥管理中心（KMC）进行规范和规定。

6.2.4 私钥备份

HNCA的CA私钥在加密机中生成，备份形式包括加密机双机备份和定期的加密导出备份。

HNCA不提供订户签名私钥备份服务。订户加密密钥对由河南省密钥管理中心（KMC）备份，其生命周期管理由河南省密钥管理中心（KMC）进行规范和规定。

6.2.5 私钥归档

HNCA在CA证书到期后对CA私钥进行归档保存，用于CA私钥恢复的密钥管理员卡也同时进行归档保存。归档期限届满后，按照本CPS的规定对私钥进行销毁处理。

HNCA不对订户提供私钥归档服务。

6.2.6 私钥导入或导出密码模块

CA私钥的导出和导入，由至少3个密钥管理员分别登录加密机，通过加密机进行加密导出和导入。

对于订户，HNCA提供将加密私钥安全传送给订户的方法，不提供订户私钥导出的方法。

6.2.7 私钥在密码模块中的存储

私钥在密码模块中加密保存。

6.2.8 激活私钥的方法

激活私钥至少需要3名密钥管理员同时在场，使用智能IC卡登录加密机，启动

密钥管理程序，进行激活私钥的操作。

6.2.9 解除私钥激活状态的方法

解除私钥激活状态至少需要3名密钥管理员同时在场，使用智能IC卡登录加密机,启动密钥管理程序，进行解除私钥的操作。

6.2.10 销毁密钥的方法

HNCA的私钥不再被使用，或者与私钥相对应的公钥到期或者被撤销后，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。销毁时由3名以上的密钥管理员共同在场，由操作员负责清空硬件加密设备，完成密钥销毁。私钥归档的操作按照本CPS的规定处理。

6.2.11 密码模块的评估

HNCA使用国家密码主管部门批准和许可的密码产品，接受其颁布的各类标准、规范、评估结果、评价证书等各类要求。根据HNCA对产品性能、工作效率、供应厂商的资质等方面的评估，选择需要的模块。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

公钥的归档，其操作过程、安全措施、保存期限以及保存策略和证书保持一致。归档要求参照本CPS中§5.5记录归档的相关规定。

6.3.2 证书操作期和密钥对使用期限

所有订户证书的有效期和其对应的密钥对的有效期都是一致的。

6.4 激活数据

6.4.1 激活数据的产生和安装

激活数据是私钥保护密码，证书存储介质（如：智能USB KEY）出厂时设置缺省的PIN值。

6.4.2 激活数据的保护

订户应及时修改证书存储介质的默认PIN值，以确保安全。

6.4.3 激活数据的其他方面

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

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

为保证系统的正常运行，对所需要的计算机设备进行正确的选型、验收，制定操作规范。另外，本系统采用增加冗余资源的方法，使系统在有故障时仍能正常工作。

对于设备有一套完整的保管和维护制度：

a) 专人负责设备的领取和保管，做好设备的领用、进出库和报废登记。

b) 对设备定期进行检查、清洁和保养维护。

c) 制定设备维修计划，建立满足正常运转最低要求的易损坏备件库。

d) 对设备进行维修时，必须记录维修的对象、故障原因、排除方法、主要维修过程及与维修有关的情况等。

e) 设备维修时，必须有派专人在场监督。

6.5.2 计算机安全评估

HNCA 电子认证服务系统已通过国家密码管理局组织的安全性审查和安全技术鉴定。

6.6 生命周期技术控制

6.6.1 系统开发控制

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

6.6.2 安全管理控制

HNCA电子认证服务系统的安全管理控制，严格遵循管理部门的有关运行管理规范和HNCA的安全管理策略进行操作。

HNCA采用严格的管理体系来保证操作系统、网络设置和系统配置安全，以防止未授权的修改。

6.6.3 生命周期的安全控制

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主管部门鉴定，使用了基于标准的强化安全通信协议确保了通信数据的安全，在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施，整个系统安全可靠。

6.7 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。HNCA采取防火墙、病毒防治、入侵检测、数据备份、灾难恢复等安全防护措施。

6.8 时间戳

HNCA电子认证服务系统不采用时间戳技术来标识系统日志和记录的时间。

7. 证书、证书撤销列表和在线证书状态协议

7.1 证书

HNCA签发的证书格式，符合《GM/T 0015-2012 基于SM2密码算法的数字证书格式规范》或ITU-T X.509 V3。

7.1.1 版本号

符合X.509 V3证书格式，这一版本信息存放在证书版本属性栏内。

7.1.2 算法对象标识符

a) 签名算法

SHA1withRSAEncryption对象标识符为：OID 1.2.840.113549.1.1.5

SHA256withRSAEncryption对象标识符为：OID 1.2.840.113549.1.1.11

SM3withSM2Encryption对象标识符为：OID：1.2.156.10197.1.501

b) 摘要算法

sha1的对象标识符为：OID 1.2.156.197.1.410

sha256的对象标识符为：OID：1.2.156.197.1.411

SM3的对象标识符位：OID：1.2.156.197.1.401

c) 非对称算法：.

RSA对象标识符为：OID 1.2.840.113549.1.1.1

SM2对象标识符为：OID 1.2.156.10197.1.301

d) 对称算法

本CPS建议使用国家密码管理部门认可的对称算法。

7.1.3 名称形式

HNCA签发的证书，其名称形式符合X.500的甄别名格式。

7.1.4 证书扩展项

HNCA证书扩展项除使用IETF RFC 3280中定义的证书标准扩展项，还支持私有扩展项。

HNCA采用的IETF RFC 3280中定义的证书标准扩展项：

a) 颁发机构密钥标识符Authority Key Identifier ；

b) 主体密钥标识符SuHNect Key Identifier ；

c) 密钥用法Key Usage ；

d) 扩展密钥用途Extended Key Usage ；

e) 私有密钥使用期Private Key Usage Period ；

f) 主体可选替换名称SuHNect Alternative Name ；

g) 基本限制Basic Constraints ；

h) 证书撤销列表分发点CRL Distribution Points 。

私有扩展项可支持以下类型：

a) 个人身份识别码Identify Card Number ；

b) 企业工商注册号IC Registration Number ；

c) 企业组织机构代码Organization Code ；

d) 企业税号Taxation Number；

e) 社保号Insurance Number。

7.2 证书撤销列表

HNCA定期签发CRL，供各参与方查询使用。

7.2.1 版本号

证书撤销列表符合X.509 V2格式，此版本号存放在CRL版本格式栏目内。

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

HNCA为订户提供OCSP（在线证书状态查询服务），OCSP作为CRL的有效补充，方便各参与方及时查询证书状态信息。

7.3.1 版本号

使用OCSP版本1（OCSP v1）。

7.3.2 OCSP 扩展项

未使用OCSP扩展项。

8. 电子认证服务机构审计和其他评估

审计评估是为了检查、确认HNCA是否按照CPS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。审计评估分内部审计评估和外部审计评估。同时，按规定接受管理部门的评估和检查。

8.1 评估的频率或情形

a）内部审计评估是由HNCA组织内部人员进行的审计评估，审计评估的结果可供HNCA改进、完善业务，内部审计评估结果不需要公开。每年至少执行一次内部审计评估，对HNCA经营管理活动进行风险识别、评估、分析、控制，整理形成《内部风险控制报告》，并针对自查中出现的问题，进行改进、完善。

b）外部审计评估由委托的第三方审计评估机构来承担，审计评估的依据包括HNCA-CPS、安全策略、业务规范、管理制度以及管理部门的相关要求及技术规范。

c）根据《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电

子认证服务密码管理办法》、《电子政务电子认证服务管理办法》的规定，接受管理部门的评估和检查。

8.2 评估者的资质

HNCA无条件接受管理部门的审计评估，评估者所具有的资质由管理部门决定。

HNCA在进行内部审计评估时，要求评估人员至少具备认证机构、信息安全审计评估的相关知识，有三年以上的相关经验，并且熟悉本CPS的规范，以及应具备计算机、网络、信息安全等方面的知识和实际工作经验。内部审计评估由企业内控部门组织实施。

HNCA在进行外部审计评估时，选择专业、公正、客观的专业审计评估机构，要求评估者具备以下的资质：

a) 必须是经许可的、有营业执照的评估机构，在业界享有良好的声誉；

b) 了解计算机信息安全体系、通信网络安全要求、PKI技术、标准和操作；

c) 具备检查系统运行性能的专业技术和工具。

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

HNCA接受管理部门依法依规提出的评估要求和内容。

HNCA内部审计评估的内容包括但不限于：

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

b) 服务的完整性：密钥和证书生命周期的安全管理、业务系统的安全操作、业务操作规范性审查。

c) 物理和环境安全控制：信息安全管理、人员的安全控制、建筑设施的安全控制、软硬件设备和存储介质的安全控制、系统和网络的安全控制、系统开发和维护的安全控制、灾难恢复和备份系统的管理、审计和归档的安全管理等。

HNCA根据实际需要确定外部审计评估内容。

8.5 对问题与不足采取的措施

对审计评估中发现的问题，HNCA将根据法律法规、行业政策、技术标准规范和自身策略制订有效的改进计划及预防措施，对落实情况进行再次评估以达到解决问题的目标。

8.6 评估结果的传达与发布

管理部门在完成评估后，按照法律法规的要求对评估结果进行处理。

除非法律明确要求，HNCA的内部和外部审计评估结果一般不公开。

9. 法律责任和其他业务条款

9.1 费用

HNCA根据市场情况和提供的电子认证服务内容确定收费标准,并向订户收取费用。

9.1.1 证书签发和更新费用

HNCA收取合理的证书签发和更新费用，并在订户订购时提前告知。

9.1.2 证书查询费用

HNCA对证书查询，目前不收取任何费用。

9.1.3 证书撤销或状态信息的查询费用

HNCA对证书撤销和状态查询，目前不收取任何费用。

9.1.4 其他服务的费用

HNCA保留收取其他服务费的权利。

9.1.5 退款策略

HNCA对订户收取的费用，除了证书申请和更新费用因为特定理由可以退还外，HNCA均不退还订户任何费用。

9.2 财务责任

HNCA 确保具有足够的财务实力来维持其正常经营并保证相应义务的履行，并合理地承担对订户及对依赖方的责任。

此要求对订户同样适用。

9.3 业务信息保密

9.3.1 保密信息范围

a) 保密信息包括HNCA与其授权的RA和合作方、HNCA与订户、HNCA与其他各参与方之间的协议、往来函和商务协定等。除非法律明确规定和HNCA明确进行了书面许可，一般不能在未经另一方许可的情况下擅自公开。

b) 订户应该遵照本CPS的规定妥善保管私钥，如果因订户泄露私钥，订户应自行承担一切责任。

c) HNCA的内部和外部审计评估结果及相关信息是机密信息，除了HNCA授权和信任的人员，不能泄露给其他任何人。这些信息除了审查目的或法律规定的目的，不能用于其他用途。

d) HNCA所有涉及系统运营的信息，都在保密范围之内。

e) 除非法律明文规定，HNCA不会公布或透露订户证书中已经包括的信息以外的任何信息；同时，HNCA在与其授权的RA和合作方或其他参与方签署协议时，都将此作为必须满足的要求。

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。HNCA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。

订户证书及撤销信息通过HNCA目录服务等方式向外公布。

9.3.3 保护保密信息的责任

HNCA或其授权的RA和合作方、订户、依赖方和其他各参与方，都有义务按照本CPS的规定，承担相应的保护保密信息的责任。

当保密信息的所有者出于某种原因，要求HNCA公开或披露他所拥有的保密信息时，应书面授权以表示其自身的公开或者披露意愿，HNCA应满足其要求。如该披露行为涉及任何其他方的赔偿义务和所造成的损失，应由保密信息的所有者承担，HNCA不予承担。

9.4 个人隐私保密

9.4.1 隐私保密方案

HNCA尊重所有订户及其隐私，个人隐私信息保密方案遵守现行法律和政策规定。

订户选择使用HNCA的服务，就表示已经同意接受HNCA有关隐私保护的声明。

9.4.2 作为隐私处理的信息

申请者提供的不构成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

申请者提供的用来构成证书内容的资料不认为是隐私信息。

证书是公开的，通过HNCA目录服务等方式向外公布。

9.4.4 保护隐私的责任

接收到隐私信息的参与者有责任保护隐私信息不被泄漏、使用或发布给第三方。

9.4.5 使用隐私信息的告知或同意

使用隐私信息，须征得本人同意。

9.4.6 依法律或行政程序的信息披露

当HNCA在任何法律法规要求或者法院以及其它公权力部门通过合法程序的要求下，必须披露本CPS中规定的保密信息时，HNCA可以按照法律法规或相关政策以及法院判决的要求，向执法部门提交相关的保密信息。HNCA不承担任何责任。这种披露不能被视为违反了保密要求和义务。

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，HNCA享有并保留对证书以及HNCA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。

按本CPS的规定，所有由HNCA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HNCA所有，这些知识产权包括所有相关的纸质和电子文档。HNCA的知识产权可以授权相关实体使用。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

HNCA在提供电子认证服务活动过程中的承诺如下：

a）HNCA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领导，对签发的证书承担相应的法律责任。

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

c）除非已通过HNCA证书库发出了HNCA的私钥被破坏或被盗的通知，HNCA保

证其私钥是安全的。

d) HNCA签发给订户的证书符合HNCA-CPS的所有实质性要求。

e) HNCA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。

f) HNCA将及时撤销证书。

g) HNCA拒绝签发证书后，将立即向证书申请人归还所付的全部费用。

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

i）HNCA 与合作方系业务合作关系，根据合作协议内容分别承担各自的责任和义务。

9.6.2 注册机构的陈述与担保

HNCA的注册机构在参与电子认证服务过程中的承诺如下：

a) 提供给订户的注册过程完全符合HNCA-CPS的所有实质性要求。

b) 在HNCA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。

c) 注册机构将按CPS的规定，及时向HNCA提交证书申请、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HNCA签发的证书，就被视为向HNCA或其授权的RA和合作方及依赖方作出以下承诺：

a) 订户需熟悉本CPS的条款和与其证书相关的政策，还需遵守订户证书使用方面的有关限制。

b) 订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，可供HNCA或其授权的RA和合作方检查和核实。

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) 私钥仅为订户本身访问和使用，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，订户应及时通知HNCA或其授权的RA和合作方，申请采取撤销等处理措施。

f）订户已知其证书被冒用、破解或被他人非法使用时，应及时向HNCA或其授权的RA和合作方申请撤销其证书。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉本CPS的条款以及和订户相关的证书政策，并确保订户的证书用于申请时预定的目的。

依赖方在信赖订户的证书前，必须采取合理步骤，验证订户证书及数字签名的有效性。

依赖方必须承认，他们对证书的信赖行为就表明他们承认了解本CPS的有关条款。

9.6.5 合作方的陈述与担保

合作方必须熟悉本CPS的条款以及和订户相关的证书政策，并根据合作协议承担相应的法律责任和义务。

9.6.6 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

有下列情况之一的，应当免除HNCA之责任：

a）如果证书申请人故意或无意地提供了不完整、不可靠或已过期的信息，又根据正常的流程提供了必需的审核文件，得到了HNCA签发的证书，由此引起的经济纠纷应由证书申请人全部承担，HNCA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。

b）HNCA不承担任何其他未经授权的人或组织以HNCA名义编撰、发表或散布的不可信赖的信息所引起的法律责任。

c）HNCA不承担在法律许可的范围内，根据受害者或法律的要求如实提供网上业务中“不可抵赖”的数字签名依据所引起的法律责任。

d）HNCA不对任何一方在信赖证书或使用证书过程中引起的直接或间接的损失承担责任。

e）HNCA或其授权的RA和合作方不是订户或依赖方的代理人、受托人、管理人或其他代表。HNCA和订户间的关系以及HNCA和依赖方间的关系并不是代理人和委托者的关系。订户和依赖方都没有权利以合同形式或其他方法让HNCA承担信托责任。

f）由于客观意外或其他不可抗力事件原因而导致证书签发错误、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§9.16.4不可抗力。

g）因HNCA的设备或网络故障等技术故障而导致证书签发延迟、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：

- 不可抗力；
- 关联单位如电力、电信、通讯部门而致；
- 黑客攻击；
- 设备或网络故障。

h）HNCA已谨慎地遵循了国家法律、法规规定的证书认证业务规则，而仍有损失产生的。

9.8 有限责任

HNCA根据与各关联实体签订的合同承担相应的有限责任。

HNCA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。

9.9 赔偿

9.9.1 HNCA 的赔偿责任范围

如因HNCA过错，发生证书信息错误、被伪造、篡改的， HNCA承担赔偿责任，范围如下：

a) 证书信息与订户提交的信息资料不一致，造成订户损失。

b) 因HNCA原因，致使订户证书无法正常使用，造成订户损失。

c) HNCA只在证书有效期限内承担损失或损害赔偿。

9.9.2 其他方的赔偿责任范围

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HNCA或其授权的RA和合作方产生损失，订户和依赖方应承担赔偿责任。

订户接受证书就表示同意在以下情况下承担赔偿责任：

a) 未向HNCA提供真实、完整和准确的信息，而导致HNCA或有关各方损失。

b) 未能保护订户的私钥，或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用，而导致HNCA或有关各方损失。

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

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

e) 证书的非法使用，即违反HNCA对证书使用的规定，而导致HNCA或有关各方损失。

9.9.3 对最终实体的赔偿担保

HNCA对所有当事实体（包括但不限于订户、依赖方）的合计责任不超过证书适用的责任封顶。对于一份证书产生的所有数字签名和交易处理，HNCA对于任何人有关该特定证书的合计责任应该限制在一个不超出赔偿责任上限的范围内。

HNCA所颁发证书的赔偿责任上限如下：

个人证书：500元人民币。

机构证书：2000元人民币。

服务器证书：8000元人民币。

HNCA 依据所提供的电子认证服务内容确定对应的赔偿责任上限，并及时予以公布。

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。HNCA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。

9.10 有效期限与终止

9.10.1 有效期限

本CPS自发布之日起正式生效。

本CPS中将详细注明版本号及发布日期。

9.10.2 终止

当新版本的CPS正式发布生效时，旧版本的CPS自动终止。

9.10.3 效力的终止与保留

CPS的某些条款在终止后继续有效，如知识产权承认和保密条款。另外，各参与方应返还保密信息到其拥有者。

9.11 对参与者的个别通告与沟通

除非法律法规或者协议有特别的规定，HNCA将以合理的方式与相关各方进行沟通，不会采取个别的方式进行。

9.12 修订

9.12.1 修订程序

当CPS不适用时，由HNCA安全策略管理委员会委托执行组对CPS进行修订，修订程序同1.5.4。

9.12.2 通告机制和期限

本CPS在HNCA网站https://www.hnca.com.cn上发布。

版本更新时，最新版本的CPS在HNCA的网站发布，对具体个人不做另行通知。

9.12.3 必须修改业务规则的情形

当管辖法律、适用标准及操作规范等有重大改变时，必须修改CPS。

9.13 争议处理

订户、依赖方等关联实体在电子认证活动中产生争端可按照以下步骤解决：

a) 当事人首先通知，根据本CPS中的规定，明确责任方；

b) 由相关部门负责与当事人协调；

c) 若协调失败，可以通过司法途径解决；

d) 任何因与HNCA或其授权的RA和合作方就本CPS所产生的任何争议而提起诉讼的，受HNCA工商注册所在地的人民法院管辖。

9.14 管辖法律

本CPS在各方面服从中国法律和法规的管制和解释，包括但不限于《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CPS的执行、解释、翻译和有效性均适用中华人民共和国的法律。

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 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。

9.16.3 强制执行

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

9.16.4 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。

在电子认证服务活动中，HNCA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者全部免除违约责任。其他认证各方（如订户）不得提出异议或者申请任何补偿。

9.17 其他条款

HNCA的安全策略管理委员会对本CPS拥有最终解释权。