HNCA电子政务电子认证服务业务规则

(版本4.0)

(生效日期：2019年9月5日)

华测电子认证有限责任公司

CTI Certificate Authority Co.,Ltd.

版权声明

HNCA电子政务电子认证服务业务规则修订表

版本	发布日期	备注
1.0	2011年5月16日	参照《电子政务电子认证服务业务规则规范》 《电子政务电子认证服务管理办法》 《电子认证服务密码管理办法》 《证书认证系统密码及其相关安全技术规范》 《电子政务数字证书格式规范》 《电子政务数字证书应用接口规范》 《中华人民共和国电子签名法》
2.0	2016年11月16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
3.0	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
4.0	2019年9月5日	根据《电子政务电子认证服务业务规则规范》进行修订

目 录

1.概括性描述

1.1 概述

HNCA电子政务电子认证服务业务规则（以下简称“HNCA E-GOV CPS”）由HNCA按照国家密码管理局《电子政务电子认证服务管理办法》的要求，依据《电子政务电子认证服务业务规则规范》制定，以规范HNCA的电子政务电子认证业务的管理,保障认证体系的安全可靠,有效防范安全风险。

HNCA严格按照《中华人民共和国电子签名法》、《电子政务电子认证服务管理办法》、《电子政务电子认证服务业务规则规范》等法律法规的要求，提供数字证书审核、签发、发布、存档和注销等证书生命周期管理及相关业务服务，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，为电子政务构建安全、可靠的信任环境。

本文档名称是《HNCA电子政务电子认证服务业务规则》,简称HNCA E-GOV CPS。本HNCA E-GOV CPS是HNCA发布的第四个版本，版本号V4.0。HNCA E-GOV CPS将会根据HNCA第三方电子政务电子认证服务的发展定期更新。

HNCA E-GOV CPS 详细阐述了HNCA在实际工作和运行中所遵循的各项规范。本规则适用于HNCA及其员工、注册机构、订户、依赖方和其他参与者。各参与方必须完整地理解和执行HNCA E-GOV CPS所规定的条款,并承担相应的责任和业务。

1.2 电子政务电子认证业务范围

1.2.1 数字证书服务

HNCA面向电子政务活动中的政务部门和企事业单位、社会团体、社会公众等电子政务用户提供的证书申请、证书签发、证书更新和证书撤销等证书全生命周期管理服务。

1.2.2 数字证书类型

各个证书代表各自的身份进行使用。所有证书根据其颁发对象的不同，归为以下三类：

- 个人证书

- 机构证书
- 设备证书

HNCA在开展业务时可能为某种对象的证书做特别命名。证书类型及用途参见HNCA网站https://www.hnca.com.cn上的介绍，证书申请者根据实际需要，决定采用哪种证书类型。

1.2.3 证书订户性质

证书类型	订户性质	范例
个人证书	各级政务部门的工作人员和参与电子政务业务的社会公众，用以代表个体身份。	某政府机关职员
机构证书	政府机关和参与电子政务业务的企事业单位，代表机构身份	参加招投标业务的投标企业
设备证书	电子政务系统中的服务器或者其他设备，用以代表设备身份的真实性	服务器身份证书

1.2.4 限制的证书应用

发放的数字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用户负责。

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》、《电子认证服务密码管理办法》、《电子政务电子认证服务管理办法》等规定，依法设立的第三方电子认证服务机构（简称CA）。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。

1.3.1.1 HNCA的根

ROOTCA是HNCA电子认证服务系统加入的国家根的名称。HNCA为最终订户签发的个人证书、机构证书和设备证书由ROOTCA为HNCA签发的CA所签发。

国家SM2算法根证书的DN为：

CN=ROOTCA

O=NRCAC

C=CN

国家根为HNCA签发的SM2根证书DN为：

CN = HNCA

O = HeNan Certificate Authority

L = ZhengZhou

S = HeNan

C = CN

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、注销和下载等业务。

HNCA本身是CA，也承担RA职责，还可以授权建立外部RA。RA应遵循本E-GOV CPS以及HNCA的授权，负责建立和管理下属业务受理点(LRA)。

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E-GOV 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。

订户符合以下情况：

- 在接受的证书中指明或识别为证书接受者；
- 已接受该证书并遵守HNCA E-GOV CPS和相关协议；
- 拥有与接受证书内公钥所对应的私钥。

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 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。

1.3.6 各方主要责任

HNCA：向订户明确办理各项业务的流程及所需材料。受理业务应严格执行身份鉴别，与订户签订相关协议，签发证书时应明确证书持有者私钥和证书的用途。向依赖方提供验证签名信息的方式。

订户：办理证书时遵循HNCA E-GOV CPS和相关协议，提供相应业务所需的材料或证明。对证书及私钥，应按照国家相关标准规范的要求妥善保管和使用。因未妥善保管私钥、未按规定用途使用证书或私钥，造成的损失由证书持有者自行承担责任。

依赖方：依赖方应按HNCA提供的方式对签名信息进行验证。未按约定方式验证签名信息造成损失的，由依赖方自行承担责任。

1.4 电子政务电子认证策略管理

1.4.1 管理机构

HNCA E-GOV CPS的管理机构是HNCA安全策略管理委员会，安全策略管理委员会下设执行组。执行组负责编写、修订E-GOV CPS。

1.4.2 联系方式

HNCA E-GOV 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；

联系部门：行政部；

邮政编码：450046；

电话号码：0371-68107818；

传真号码：0371-68107808。

1.4.3 批准程序

1）起草小组成立流程

HNCA E-GOV CPS的编写和修订由安全策略管理执行组负责，安全策略管理执行组成员由安全策略管理委员会任命。

2）HNCA E-GOV CPS的审批流程

安全策略管理执行组起草E-GOV 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。

3）发布流程

安全策略管理执行组提交修改后的E-GOV CPS到公司行政部门；公司行政部门确定E-GOV CPS文本格式和版本号，形成定稿，报总经理审批；总经理审批同意后，方可对外发布。

4）向主管机关备案流程

HNCA E-GOV CPS 从对外公布之日起三十日之内，由行政部门向国家密码管理局备案。

1.5 定义和缩写

下列定义适用于本HNCA E-GOV CPS：

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

PKI是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。

2)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。

3)电子认证服务机构（CA）Certification Authority

受订户信任，负责创建和分配公钥证书的权威机构。

4)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者，同意或拒绝证书申请，在某些环境下主动撤销证书，处理用户撤销其证书的请求，同意或拒绝用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)。

5)KMC(Key Management Center)

密钥管理中心的简称。用于产生订户加密证书密钥对，并提供加密密钥对托管服务的管理机构。

6)数字证书(证书)Digital Certificate

也称公钥证书，由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

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

一个经电子认证服务机构数字签名的列表,它指定了一系列证书颁发者认为无效的证书，也称黑名单服务。

8)机构撤销列表（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CA机构证书已经无效。

9)私钥(电子签名制作数据) Private Key

指在电子签名过程中使用的,将电子签名与电子签名人可靠地联系起来的字符、编码等数据。

私钥是经由数字运算产生的密钥，用于制作电子签名数据，亦可依据其运算方式，就相对应的公开密钥加密的文件或信息予以解密。

10)公钥(电子签名验证数据) Public Key

公钥是经由数字运算产生的密钥，用于解密电子签名，确认电子签名人的身份及电子签名的真实性。

公钥可以公开，一般标示于在线数据库、存储库或其他公共目录中，使任何希望得到公钥的人都能得到。

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、算法或者公钥等。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。

11)OCSP (Online Certificate Status Protocol)

在线数字证书状态查询协议的简称,用于支持实时查询数字证书状态。

12)LDAP（Lightweight Directory Access Protocol）

轻量级目录访问协议的简称。LDAP用于查询、下载数字证书以及数字证书注销列表（CRL）。

13)RSA算法

RSA是由 Rivest、 Shamir及 Adelman 所发明的一种公开密钥加密算法，以数论的欧拉定理为基础，它的安全性依赖于大数的因数分解的困难性。

14)SM2算法

SM2算法是基于国际ECC算法的一种椭圆曲线公钥密码算法。

15)X.509

一种由ITU-T(International Telecommunication Union-T:国际电信联盟）所发布的数字证书标准以及对应的验证架构。X.509 v3则为一种具扩展栏位或可扩展的数字证书。

1.6 信息发布与信息管理

1.6.1 信息库

HNCA信息库是一个对外公开的信息库，能够保存、取回证书及与证书有关的信息。HNCA信息库内容包括但不限于以下内容：证书、CRL、E-GOV CPS、电子认证服务协议、HNCA不定期发布的信息。主要为订户和网络应用提供HNCA证书查询及验证证书状态服务的资料库。HNCA信息库不会改变任何从发证机构发出的证书和任何证书注销的通知，而是准确描述上述内容。

HNCA通过网站公布以下信息：HNCA E-GOV CPS发布在HNCA网站上，HNCA网站为https://www.hnca.com.cn（本文中“HNCA网站”均指此网址）。

HNCA 通过目录服务器发布订户的证书和 CRL，订户或信赖方可以通过访问 HNCA 的目录服务器获取证书的信息和 CRL。同时，HNCA 提供在线证书状态查询服务。

除 HNCA 授权者外，禁止访问信息库（或其它由 CA 或 RA 维护的数据）中任何被 E-GOV CPS 或 HNCA 信息库宣布为机密信息的资料。

1.6.2 认证信息的发布

1） E-GOV CPS的发布

HNCA E-GOV CPS 一经在 HNCA 网站或以书面声明形式发布、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。HNCA E-GOV CPS 的发布及更改遵循本文 1.4 的规定。可访问 HNCA 网站查看，对具体个人不另行通知。

2） 证书和CRL发布

数字证书在签发成功后，HNCA将该证书副本发布到信息库。HNCA定期发布CRL以公布在证书有效期内被注销的数字证书。证书依赖方可在HNCA的LDAP服务器或其他指定的信息库位置中查询获得证书和CRL有关信息。同时，HNCA也提供标准的OCSP服务，证书依赖方经授权可实时地获取证书最新的状态信息。

1.6.3 发布时间或频率

1） E-GOV CPS的发布时间或频率

HNCA定期对E-GOV CPS进行评估，如有修改、补充、调整等，HNCA将及时在HNCA网站发布。

HNCA根据技术进步、业务发展、应用推进和法律法规的客观要求，决定对E-GOV CPS的改动，其发布时间和频率将由HNCA独立做出决定。

在HNCA没有发布新的E-GOV CPS或没有任何形式的公告、通知等形式宣布对E-GOV CPS进行修改、补充、调整或更新前，当前的E-GOV CPS即处在有效的和正在实施的状态。

2） 证书的发布时间或频率

数字证书在签发成功后，HNCA最迟24小时内将该证书副本发布到信息库。订户也可以在其它信息库中公布其获得的HNCA签发的证书。

HNCA 通过目录发布服务和指定的信息库位置定期发布更新的数字证书信息。订户和依赖方可在HNCA的LDAP服务器或指定的信息库上查询、下载数字证书。

3) CRL的发布时间或频率

HNCA会在每批次注销证书后，签发最新CRL并发布到HNCA的LDAP服务器或指定的信息库位置。从证书被注销，到反映该证书状态的最新CRL发布的最大延迟不超过24小时。

1.6.4 信息库访问控制

HNCA在其网站上发布与其相关的公众信息。通过设置访问控制和安全审计措施，确保只有授权的 HNCA 工作人员才能编写、修改和删除HNCA在线发布的信息资料。同时，HNCA在必要时可自主选择是否实行信息的权限管理，以确保只有数字证书订户才有权阅读受 HNCA 权限控制的信息资料。

对于HNCA发布的E-GOV CPS、CRL和证书信息，证书订户和证书依赖方可以不受限制地进行只读访问，HNCA允许公众自行通过网站和目录服务器进行查询和访问。

只有经授权的RA/CA管理员可以查询电子认证服务机构和注册机构数据库中的其他数据。

2.身份标识与鉴别

2.1 数字证书命名与格式

2.1.1 证书命名

数字证书命名应遵循GM/T 0015的要求，不得使用匿名或假名。每张数字证书都包含有主体(Subject)，目的是标识该证书由谁持有。这些主体的命名方法采用X.501的甄别名(Distinguished Name,简称 DN)方式。DN通常包含以下部分或其部分：

•C，国家

•S，所在省、市等行政区

•L，地址

•O，组织

•OU，组织下的部门或分支

•CN，主体名称

•E，电子邮件

不同证书类型的DN的取值和编排方式有所不同，并且所有证书涉及命名的内容都经过严格审核，DN应遵循以下原则：

1）DN必须是唯一的。

2）DN必须能明确标识订户的真实身份；

3）应结合主体名称、电子邮箱、地址等信息，唯一标识客观实体。

2.1.2 证书版本

HNCA签发的证书为X.509标准数字证书，证书中可查看版本信息。

2.1.3 证书扩展项

HNCA 支持 GM/T 0015 标准中指定的标准扩展，还支持私有扩展项。

HNCA 证书支持的标准扩展包括：

颁发机构密钥标识符 Authority Key Identifier

主体密钥标识符 SuHNect Key Identifier

密钥用法 Key Usage

扩展密钥用途 Extended Key Usage

私有密钥使用期 Private Key Usage Period

主体可选替换名称 SuHNect Alternative Name

基本限制 Basic Constraints

证书撤销列表分发点 CRL Distribution Points

私有扩展项可支持以下类型：

个人身份识别码 Identify Card Number

企业工商注册号 IC Registration Number

企业组织机构代码 Organization Code

企业税号 Taxation Number

社保号 Insurance Number

2.2 身份标识与鉴别

2.2.1 证明持有私钥的方法

签名私钥由证书申请者生成，属于证书申请者专有；

证书申请者应使用其私钥对证书请求信息进行数字签名

CA使用证书申请者公钥验证证书请求中所包含的数字签名，来证明证书申请者持有与注册公钥对应的私钥。

证书申请者作为其私钥的唯一持有者，对自己的私钥的保管应符合GM/T 0034和GM/T 0028等相关标准规范。

2.2.2 组织机构身份鉴别

HNCA通过证书申请者提交申请材料的方式获取证书申请者信息。HNCA通过查验能证明其机构身份的证件的原件，或通过第三方信息数据或服务，或电话访问等HNCA认为恰当的查验方式来确定机构的身份是确实存在的、合法的实体。

同时，HNCA也需对经过机构授权办理证书业务的代表的身份进行确认，确定该机构知晓并授权证书申请。如该企业需申请服务器类型的证书，还需向注册机构提交域名证明文件。

如果HNCA或其授权的RA和LRA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、LRA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、LRA应确保申请者的身份鉴别材料或电子数据具备不可篡改和抗抵赖性，并妥善保存。

2.2.3 个人身份的鉴别

申请者应提交个人身份证明材料，以确认个人的身份是确实存在的、合法的实体。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。

如果证书申请者委托他人代为提交申请，HNCA还应对代理人的身份进行验证，并确认证书申请者知晓并授权证书申请，代理人提交证书申请是经过授权的。

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

对于特定环境中使用的个人身份，HNCA可以在对依赖方的身份审核机制评估通过后，授权依赖方负责收集和鉴别个人身份并代理个人向HNCA或其授权的RA、LRA发起证书申请。

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、LRA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、LRA应确保申请者的身份鉴别材料或电子数据具备不可篡改和抗抵赖性，并妥善保存。

2.2.4 政府部门个人身份的鉴别

在按照个人身份鉴别要求进行外，还需要：

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。

2.2.5 不予验证的订户信息

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。

2.2.6 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数字证书事宜的授权文件。

机构在HNCA的数字证书登记表上加盖单位公章后，则证明本组织对办理人的授权确认。

2.3 密钥更新请求的身份鉴别

在密钥更新中，需要经过身份审核，才能够完成更新过程。

HNCA可以采用以下方式来对更新证书的订户身份进行鉴别：

1）持有有效证书的订户现场进行密钥更新申请，订户可选择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，也可选择使用与初始身份确认相同的鉴别流程。

2）订户证书已过期时，应重新进行与初始身份确认相同的鉴别流程。

3）在线更新方式，仅支持持有有效证书的订户，订户应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。

2.4 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，证书申请应重新进行与初始身份确认相同的鉴别流程。

3.证书生命周期操作要求

3.1 证书申请

3.1.1 证书申请流程

1）证书申请者从HNCA或其授权的注册机构获取相应种类的数字证书申请登记表格，也可从HNCA网站上下载打印，按表格要求填好申请表。

2)证书申请者向HNCA及其授权的注册机构提交申请信息，也可通过 HNCA 的在线服务系统提交申请信息。

3）HNCA或其授权的注册机构根据申请者提交的资料进行鉴别，完成后进行注册、审核和交费等。

3.1.2 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。

3.1.3 注册过程与责任

证书申请者按照 HNCA E-GOV CPS 所规定的要求，填写证书登记表，并准备相关的身份证明材料。HNCA或其授权的注册机构依据§2.2初始身份确认验证方法对证书申请者的身份进行鉴别，并决定是否受理申请。

申请过程中各方责任为：

- 证书申请者要按照HNCA E-GOV CPS 的要求准备证书申请材料，并确保申请材料真实准确。
- HNCA或其授权的注册机构负责接收证书申请者的请求材料，当面对订户所提供的证书申请信息与身份证明材料的一致性进行查验，并保证所有证书申请者明确同意相关的证书申请协议。完成后由HNCA保留最终的证明材料和确认信息。
- HNCA在此过程中确保证书申请信息安全传输。

3.2 证书申请处理

3.2.1 执行识别与鉴别功能

HNCA或其授权的注册机构收到证书申请者的证书申请后，按照HNCA E-GOV CPS所规定的身份鉴别流程对证书申请进行身份鉴别。具体的鉴别流程详见§2.2。

3.2.2 证书申请批准和拒绝

HNCA或其授权的注册机构对已通过身份鉴别的证书申请，根据申请内容完成费用相关流程，之后批准证书申请，向HNCA提交证书签发请求。

证书申请者未能通过身份鉴证、未在约定时间内完成费用相关流程或未满足HNCA其他申请要求条件的，HNCA 或其授权的注册机构将拒绝证书申请，并在2个工作日内通知申请者，同时向申请者提供失败的原因（法律禁止的除外）。

被拒绝的证书申请者可以在准备正确的材料后，再次提出申请。

3.2.3 处理证书申请的时间

一般情况下，HNCA收到证书申请后，将在申请者最后一次提交、补充或修改申请信息的2个工作日内处理证书申请。双方另有约定时限的情况按约定时限处理。

3.2.4 告知申请的结果

证书申请批准后，HNCA将根据申请内容进行后续业务流程，办理签发服务。如果申请被拒绝，HNCA将在2个工作日内通过适当的方式通知证书申请者。

3.3 证书签发

3.3.1 证书签发中注册机构和认证机构的行为

HNCA 将根据接受的证书申请所提供的信息来为申请实体签发证书。签发过程中，CA 与其RA之间通过可靠的安全连接方式进行身份认证及数据传递，保证信息传输的机密性。

CA 在确认为证书申请提交签发请求的 RA的身份后，验证RA的签发请求，无误后正式为申请实体签发证书。在签发过程中，HNCA 依然可以对系统记录的申请信息给予再次审核，无论是通过信息再审核或其他可靠信息渠道，如 HNCA 认为申请信息存在有任何疑点，将暂停签发证书，并通知接受申请的RA，直至澄清问题，再重新启动证书签发程序。

证书签发后，由 RA 作相应的后续处理，包括为订户将证书安装在指定的载体中并进行证书发放，或通知订户自行下载安装。

通常，HNCA所签发的证书在24小时内生效。

3.3.2HNCA 及其授权的注册机构对用户的通告方式

HNCA通过注册机构，对订户的通告有以下几种方式：

- 通过面对面的方式；
- 网站公告或电话通知；
- 邮政信函或电子邮件通知订户；

- 其他认为安全可行的方式通知订户。

3.3.3 证书获取方式

订户获取证书有如下方式：

- 由HNCA 或其授权的注册机构将证书安装在指定的载体中，直接交给订户。
- 由HNCA 或其授权的注册机构将证书安装在指定的载体中，采取合适的方式递送给订户。
- 由HNCA 或其授权的注册机构将证书获取方式及获取所需信息，采取合适的方式通知或递送给订户，由订户自行获取。

3.4 证书接受

3.4.1 构成接受证书的行为

数字证书签发完成后，根据不同的业务操作流程，HNCA或其授权的注册机构提供安全可靠的渠道，使证书申请者可以获取数字证书，满足约定方式的条件，应当视为证书申请者接受证书。

3.4.2 认证机构对证书的发布

HNCA在签发完证书后，就将证书发布到数据库和目录服务器中。订户或依赖方拒绝发布证书信息的，应明确向认证机构提出，由认证机构根据订户或依赖方的意愿，发布或者不发布证书信息。

3.4.3HNCA 在颁发证书时对其他实体的通告

除订户和HNCA授权的注册机构外，HNCA不需要通知其他实体证书的签发。其他实体可以通过HNCA目录服务器查询到HNCA已经发布的数字证书。

3.5 密钥对和证书的使用

3.5.1 订户私钥和证书的使用

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

HNCA通过证书内容、与订户和依赖方约定等方式限制了证书及对应私钥的用途，订户只能在指定的应用范围内、按约定的方式使用证书及对应私钥。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撤销之后，订户必须停止使用证书及对应私钥。

未按上述要求使用证书及对应私钥造成损失的，由订户自行承担责任。

3.5.2 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，应通过查看证书了解其身份，并通过公钥验证对方证书的有效性。验证证书的有效性包括三个方面的内容：

- 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。
- 检验证书的有效期，确认该证书在有效期之内。
- 查询证书状态，确认该证书没有被注销。

在验证电子签名时，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。

依赖方应使用接收方的公钥进行信息加密，公钥证书应同加密信息一同发送给接收方。

3.6 证书与密钥更新

3.6.1 密钥更新的情形

证书密钥更新是指订户生成一对新密钥，并申请更新原有证书中的公钥为新的公钥，其他订户相关信息保持不变。HNCA将同时更新证书和密钥。

主要有以下情形：

1)证书的有效期将要到期；

2)因私钥泄漏申请更新；

3)证书无法继续获得信任；

4)证书无法正常使用；

5)证书丢失；

6)订户自主提出更新；

7)HNCA因法律法规、行业政策或自身策略要求更新。

被撤销或已过期的证书不能进行密钥更新。

3.6.2 证书更新的情形

证书更新通常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，为订户延长证书有效期。

出于安全原因，HNCA不支持证书发生任何变更时仍使用原有公钥。HNCA使用证书密钥更新过程来处理订户的证书更新请求，证书更新业务规则参照密钥更新执行。

3.6.3 更新申请的提交

证书持有者、证书持有者的授权代表（如：机构证书等）或证书对应实体的拥有者（如设备证书等）可以提交更新申请。

3.6.4 更新申请的鉴别

注册机构对申请证书更新的订户进行查验与鉴别，鉴别要求同本文§2.3。

3.6.5 密钥更新方式

处理更新请求可以采用两种方式：

一种方式是在线自动更新。对于持有有效证书的订户，在获得HNCA授权后，可自助进行在线证书更新操作，获得新证书。

另一种方式是人工方式更新。由HNCA或其授权的注册机构来处理证书更新请求，进行查验与鉴别，为订户制作新的证书。

3.6.6 通知订户密钥更新

在线自动更新方式，在自动完成更新、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，新证书已颁发。

人工更新方式，对订户的通告与本文§3.3.2规定相同。

3.6.7 构成接受密钥更新的行为

密钥更新后订户的证书接受与本文§3.4.1规定相同。

3.6.8HNCA 对密钥更新的发布

密钥更新的发布与本文§3.4.2规定相同。

3.7 证书变更

证书变更是指证书订户的关键信息发生变化，订户要求认证机构对已签发的数字证书进行证书信息变更。证书变更的操作流程需按照证书申请的身份鉴别和受理流程执行。

3.7.1 证书变更的情形

订户因其信息发生变化由其或其授权代表提出证书的变更申请。这些信息可以是：主体名称、主体身份ID、所属机构、住址、电子邮件、联系电话、通信地址、邮政编码等。

3.7.2 证书变更的申请

证书变更的申请与本文§3.1相同。

3.7.3 证书变更的鉴别

证书变更的鉴别与本文§3.2相同。

3.7.4 证书变更受理方式

证书持有者可以向HNCA及其授权的注册机构提交证书变更申请信息。

3.7.5 通知订户证书变更

证书变更对订户的通知同§3.3.2。

新证书签发后原证书将被撤销，24 小时内通过 CRL 发布。

3.7.6 构成接受证书变更的行为

密钥更新后订户的证书接受与本文§3.4.1 规定相同。

3.7.7HNCA 对变更证书的发布

变更证书的发布同§3.4.2。

3.8 证书撤销

3.8.1 证书撤销的情形

认证机构、注册机构及证书持有者在发生下列情形之一时，应申请撤销数字证书：

1）政务机构的证书订户不从事原岗位工作；

2）司法机构要求撤销订户证书；

3）证书订户提供的信息不真实；

4）证书订户没有或无法履行有关规定和义务；

5）HNCA、HNCA 授权的注册机构或最终证书订户有理由相信或强烈怀疑一个证书订户的私钥安全已经受到损害；

6）政务机构有理由相信或强烈怀疑其下属机构证书、人员证书、或设备证书的私钥安全已经受到损害；

7）与订户达成的证书持有者协议已经终止；

8）订户或其所属组织机构或证书使用唯一依赖方请求撤销其证书。

3.8.2 可以发起请求撤销证书的实体

当出现符合证书撤销条件中的情形时，订户、认证机构、注册机构、订户所属的组织机构或证书使用唯一依赖方有权发起证书撤销申请。

3.8.3 证书撤销的申请

证书撤销的申请与本文§3.1相同。

3.8.4 证书撤销的鉴别

证书撤销的鉴别与本文§3.2相同。

3.8.5 证书撤销受理方式

订户可以向HNCA及其授权的注册机构提交证书撤销申请信息。

3.8.6HNCA 处理撤销请求的时限

订户提交的撤销申请信息，经HNCA经过鉴别审核，确认符合条件，HNCA将在24小时内撤销证书并发布到证书撤销列表。

3.8.7 通知订户证书撤销

证书撤销对订户的通知同§3.3.2。

3.8.8 构成接受证书撤销的行为

HNCA 通知订户证书撤销，或订户未在提交撤销请求之后的 24 小时内明确对已提交的撤销请求提出异议，即视为订户接受证书撤销。

3.8.9 HNCA 对证书撤销的发布

任何时候证书被撤销，HNCA在24小时内将该信息发布到HNCA信息库，并重新签发CRL。包含该撤销证书状态的CRL最迟在24小时内可以通过证书列明的URL或者HNCA提供的其他途径获取。

当撤销的证书过期时会被从下次发布的CRL中撤出。

3.8.10 CRL 发布频率

HNCA发布CRL的最长间隔不超过24小时。

3.8.11 CRL 发布的最大滞后时间

证书从撤销到发布到CRL上的滞后时间不超过24小时。

HNCA对签发的CRL进行备份，最长时间间隔不超过24小时，备份保存时间不少于证书失效后10年。

3.8.12 在线状态查询的可用性

HNCA提供证书状态在线查询服务，并提供7×24小时查询服务。

3.8.13 在线状态查询要求

使用HNCA提供的证书状态在线查询服务，需要查询者提供所要查询证书对应的签名证书序列号和对应的HNCA根证书。

3.8.14 依赖方检查证书状态的要求

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：

1）CRL查询：利用证书中标识的CRL地址或与HNCA约定的其他CRL获取途径，下载CRL到本地，进行证书状态的检验。

2）OCSP查询：利用HNCA提供的证书状态在线查询服务，安装HNCA声明的方式查询证书状态，HNCA对符合要求的请求信息返回查询结果给请求者。

注意：依赖方要验证CRL的可靠性和完整性，确保是经HNCA发布并且签名的。

3.9 密钥生成、备份与恢复

3.9.1 密钥生成和备份

HNCA颁发的订户证书中，含有签名用途的密钥对由订户的密码设备（如智能密码钥匙或智能IC卡）或在符合GM/T 0034和GM/T 0028的密码模块中生成。而加密用途的密钥对则由河南省密钥管理中心（以下简称KMC）的密钥管理基础设施提供密钥管理服务。

3.9.2 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§2.2身份验证所述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。

4. 应用集成支持与信息服务操作规则

4.1 服务策略和流程

HNCA 提供软件应用集成和产品应用集成服务，其订户一般为组织机构(包括但并不限于党政机关、企事业单位、社会团体等）。HNCA 在应用集成范围内，可为订户提供相应的信息服务。服务规则如下：

1）HNCA 制定证书应用实施的管理策略和流程，对业务系统进行充分调研，指导或参与业务系统证书应用部分的开发和实施；

2）制定项目管理制度，规范系统和程序开发行为；

3）制定安全控制流程，明确人员职责；

4）实施证书软件发布版本管理，并进行证书应用环境控制；

5）项目开发程序和文档等资料应妥善归档保存。

4.2 应用接口

4.2.1 密码设备调用接口

HNCA 密码设备调用接口包括服务器端密码设备和客户端证书介质（如：USBKey）的底层应用接口。

服务端密码设备接口，符合 GM/T 0018 的要求。客户端证书介质的底层应用接口符合 GM/T 0016 和 GM/T 0017 的要求。

订户应遵循上述规范以及 HNCA 提供的设备配套说明、手册、集成示例、演示 DEMO 等进行接口调用。未按照设备相关说明操作，造成损失的由订户自行承担。

4.2.2 密码模块安全技术接口

HNCA 采用新模式与新技术密码模块提供的安全技术接口，符合 GM/T 0028 和 GM/T 0054 的要求。

4.2.3 通用密码服务接口

HNCA 为各类密码服务层和应用层提供统一的通用密码服务接口，符合 GM/T 0019 的要求。

4.3 集成内容

HNCA 为电子政务应用单位提供证书应用接口程序集成工作，可包括以下服务：

1）证书应用接口的开发包（包括客户端和服务器端）；

2）接口说明文档；

3）集成演示 Demo；

4）集成手册；

5）证书应用接口开发培训和集成技术支持；

6）协助应用系统开发商完成联调测试工作。

4.4 信息服务内容

HNCA 向应用集成服务订户提供相应的信息服务。

4.4.1 证书信息服务

HNCA 可向订户提供与其相关的证书签发、更新、补办等业务信息实时或定时同步服务，信息内容包括但不限于业务类型、认证机构身份标识、用户基本信息、用户证书信息等。

4.4.2CRL 信息服务

HNCA 定时发布 CRL，最长周期不超过 24 小时。

4.4.3 服务支持信息服务

HNCA 向订户或依赖方提供或发布与其相关的信息服务，包括业务规则和常见问题解答等。

4.4.4 决策支持信息服务

HNCA 向电子政务应用单位、政府监管机构提供决策支持信息，可包括用户档案信息、投诉处理信息、用户满意度信息、服务效率信息等。

4.5 信息服务管理规则

4.5.1 信息保密

HNCA 在提供信息服务过程中，根据与订户约定，对包括并不限于以下信息采取严格的保密措施：

1）个人隐私信息；

2）商业机密；

3）政府部门的敏感信息和工作秘密。

CRL 信息、订户未按约定申请不发布的证书信息不在保密范围内。

HNCA 对以上保密信息的访问进行严格的权限控制，对象包括内部工作人员、应用单位管理人员、问责取证人员、监管部门，任何访问均应根据相关规定执行相应流程并获取权限后进行。

4.5.2 信息采集

HNCA 仅在证书生命周期管理和发放过程中收集订户或证书申请者的私有信息。HNCA 仅收集证书申请者提交的鉴别信息，或与订户约定范围内的信息。

4.5.3 信息使用

HNCA 仅使用 CA 或者 RA 收集的信息。未得到业务应用单位的许可，HNCA 不使用其他相关私有信息。

4.5.4 信息安全存储

HNCA 对收集到的信息采取安全手段进行存储，确保不发生泄露、未授权访问等事件。

4.5.5 个人信息发布

HNCA 仅能面向应用集成服务订户或其所属单位发布与之相关的私有信息，以协助订户或其所属单位进行证书业务管理。

任何特定的私有信息发布应遵照相关法律和政策实行。

4.5.6 所有者纠正信息的机会

HNCA 允许订户在其证书生命周期内对其私有信息进行更正。

4.5.7 对司法及监管机构发布私有信息

HNCA 在以下情况下，可以执行将私有信息提供给获得相应授权的人员：

1）司法程序；

2）经私有信息所有者同意；

3）按照明确的法定权限的要求或许可。

4.6 信息服务方式

4.6.1 证书信息同步服务

HNCA 以接口形式提供证书信息同步服务，为了保证数据传输的安全性，HNCA 提供数字签名或其他安全策略，以防止数据在传输中被篡改或损坏。订户也可通过 HNCA 信息库获取其相关证书信息。

4.6.2CRL 信息同步服务

HNCA 一般通过接口形式提供 CRL 信息服务，为了保证数据传输的安全性，HNCA 提供数字签名或其他安全策略，以防止数据在传输中被篡改或损坏。订户也可通过 HNCA 信息库获取 CRL 发布信息。

订户、依赖方及其信息系统在获取 CRL 后，应使用 HNCA 根证书链验证 CRL 签名的有效性。

4.6.3 服务支持信息服务

HNCA 通过 WEB 网站等面向电子政务订户发布如下信息：

1）电子政务电子认证服务业务规则；

2）证书生命周期服务流程及相关费用；

3）证书用户操作手册；

4）证书常见问题解答（FAQ）；

5）获得证书帮助联系方式（用户服务方式、办公地址、邮政编码、投诉电话等）；

6）其他相关信息。

认证机构通过 WEB 网站面向电子政务应用系统集成商发布如下信息：

1）数字证书应用接口软件包；

2）数字证书应用接口实施指南；

3）证书常见问题解答（FAQ）；

4）获得证书帮助联系方式（用户服务方式、办公地址、邮政编码、投诉电话等）；

5）其他相关信息。

认证机构通过 WEB 网站面向电子政务应用系统发布如下信息：

1）时间戳服务数据接口；

2）HTTP 协议的 CRL 发布服务接口；

3）LDAP 协议的 CRL 发布接口；

4）LDAP 协议的证书发布接口；

5）OCSP 服务接口。

4.6.4 决策支持信息服务

HNCA 通过页面或接口提供通用的证书数据统计用于决策支持，应用集成过程中根据约定，也可通过接口提供适当的决策支持信息服务，如：用户档案信息、投诉处理信息、用户满意度信息、服务效率信息等。

5. 使用支持服务操作规则

5.1 服务内容

使用支持服务是 HNCA 面向订户及证书应用单位提供的一系列售后服务及技术支持工作。

5.1.1 面向证书持有者的服务支持

服务内容包括：数字证书管理、数字证书使用、证书存储介质使用以及电子认证服务支撑平台使用和应用过程中的所有问题。

5.1.2 面向应用提供方的服务支持

电子认证软件系统使用：如业务受理、LDAP、OCSP 等使用支持问题。

电子签名服务中间件的应用：解决服务中间件在集成时出现的各种情况，如客户端平台适应性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等。

5.2 服务方式

5.2.1 座席服务

订户拨打 HNCA 服务热线，通过语音系统咨询证书应用问题，热线座席根据订户的问题请求，查询系统知识库清单，协助订户处理。

5.2.2 在线服务

在线服务通过提供自助信息查询、网络实时通讯、远程终端协助，以及在线帮助与传统模式的结合，满足用户多种服务帮助的需求。

5.2.3 现场服务

根据用户的实际需求，由技术支持工程师上门现场为用户处理数字证书应用中存在的问题。

5.2.4 满意度调查

通过多种订户可接受的调查方式进行用户回访，包括电话、WEB 网站、邮件系统、短信、传真等。

向订户提供调查表格以供用户填写，调查表格应清晰载明此次回访的目的及内容，并将订户回访中产生的相关文档进行归档、保存。

5.2.5 投诉受理

HNCA 通过 WEB 网站公布电子政务电子认证服务监管部门的投诉受理方式，通过电话、网站平台、电子邮件、即时通讯工具等方式及时接受用户投诉，投诉受理过程中应记录投诉问题，并将结果及时反馈给用户。

HNCA 将投诉受理中产生的相关文档进行归档、保存。

5.2.6 培训

培训方式以 HNCA 与订户双方约定的形式开展。

培训内容主要包括：电子认证服务基础性技术知识、服务规范、证书应用集成规范及相关帮助文档、常见问题解答（FAQ）、操作手册等。

5.3 服务质量

HNCA 提供 7×12 小时的座席服务、在线服务，5×8 小时现场服务。

HNCA 对技术问题和技术故障按照一般事件、严重事件、重大事件进行分类，并制定响应处理流程和机制，以确保服务的及时性和连续性。

HNCA 接受国家密码管理局和省级密码管理部门组织开展的服务质量评估检查。

6.认证机构设施、管理和操作控制

6.1 物理控制

6.1.1 场所区域与建筑物

HNCA 机房的选址和建设按照《电子政务电子认证基础设施建设要求》，避开易发生火灾危险程度高的区域、有害气体来源以及存放腐蚀区域；避开易燃、易爆物品的地方；避开低洼、潮湿、落雷区域和地震频繁的地方；避开强振动源和强噪音源；避开强电磁场的干扰；避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁；避开重盐害地区，将其置于建筑物安全区内。

HNCA 的主机房根据业务功能划分为 KMC 区、核心区、服务区、应用业务区、管理区、配电室。各功能区域对应的安全等级和要求逐级提高，并在核心区、KMC 区设置屏蔽室保护机密数据的存储和 CA 签名密钥的使用安全，至少每五年进行一次屏蔽室检测。机房的建设和管理将严格按照国家标准及 HNCA 的规定要求执行。

6.1.2 物理访问

HNCA 将功能区域按低到高划分为不同的 KMC 区、核心区、服务区、应用业务区、管理区、配电室。采用高安全性的监控技术，包括 7*24 小时全天候动态监控的摄像机，双因素控制、可控权限和时间的门禁系统等监控技术；人工监控管理，所有进入高一级的区域，必须首先获得低一级区域的访问权限。

HNCA 设置双因素门禁系统来提高访问授权的安全性，并在进入服务、核心区时采用双人控制策略。

HNCA 制定安全策略，严格监督和监控人员访问，定期对 CA 设施的访问权限进行内审和更新，并及时跟进违规进出 CA 设施物理区域的事件。对于无权限人员，只有按 HNCA 安全策略规定，经相关安全管理人员批准授权，才可进入相应限制区域活动。所有进出机房人员的一切活动皆由摄像监控设备及系统监控软件记录。这些记录在确认无安全用途后，才可专项销毁。

6.1.3 电力和空调

HNCA 系统由双路市电电源供电，当单路电源发生故障时也能及时自动切换，提供紧急供电，维持系统正常运转；同时备有不间断电源（UPS），避免电压波动。

HNCA 系统的空调系统使用机房专用精密空调，达到机房温度和湿度的控制要求。HNCA 对于电源和空调系统的要求，严格按照国家机房管理相关规定，并且定时对系统进行检查，确保其符合设备运行要求。

6.1.4 水患防治

HNCA 机房采用符合国家标准的防水材料建造。机房内布置有防水检测系统，发现水害可以及时报警。

6.1.5 火灾预防和保护

HNCA 机房设置火灾自动报警系统和灭火系统，火灾报警系统包括火灾自动探测、区域报警器、集中报警器和控制器等，能够对火灾发生区域以声、光等方式发出报警信号，并能以自动或手动的方式启动灭火设备。

6.1.6 介质存储

HNCA 对存储有各类软件、运营数据和记录的各类介质妥善控制和保管。这些介质都会被存放在结构坚固的保险柜中，并对存放的地点设置安全保护，防止诸如潮湿、磁力、灾害以及人为可能造成的危害和破坏，同时记录介质的使用、库存、维修、销毁事件等。

6.1.7 废物处理

对于存储或记录有敏感信息的介质，包括纸张、磁盘、磁带、光盘、加密设备等，HNCA 在它们作废前或保存期满后进行销毁。HNCA 制定相关的销毁程序，按信息不可恢复的原则，对敏感数据应物理销毁或进行安全覆盖。

6.1.8 异地备份

HNCA 采用同城异地备份机制，对用于 CA 系统恢复的相关软件、CA 密钥和日常的业务数据等进行备份，以便 CA 系统在受到灾难性毁灭时能够启动灾难恢复程序恢复服务。

6.1.9 入侵侦测报警系统

HNCA 在 CA 机房内部署了入侵红外报警系统，并进行安全布防。

6.2 操作过程控制

6.2.1 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：

1)安全管理员

安全管理员对数字认证中心的物理、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。

2)系统审计员

审计人员控制、管理、使用安全审计系统，安全审计系统分布于证书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。

3)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。

4)系统管理员

系统管理员负责对证书系统的管理和业务操作，根据需要签发服务器证书和下级操作员证书，根据岗位负责不同的证书业务操作。

5)运营管理员

CA运营管理人员负责对证书服务体系在本单位的系统进行日常监控，执行系统级别的管理和维护。

6.2.2 可信角色的识别与鉴别

所有担任可信角色的人员需持有经授权的智能门禁识别卡或指纹进入相应的活动区域，或经批准后在有进入该区域权限的可信人员的陪同下进入。可信角色在业务系统内操作，应持有经授权的智能 IC 卡和证书进入系统进行相应业务的操作和管理。

6.2.3 职责需分离的角色

需要进行职责分割的角色，包括但不限于下列人员：

1)数据库管理人员和业务系统管理人员；

2)数据库管理人员和操作系统管理人员；

3)各业务系统的操作人员和审计人员；

4)证书业务录入人员和审核人员；

5)负责密钥及密码设备管理人员和操作人员。

6.3 人员控制

6.3.1 可信人员要求

所有员工与 HNCA 签订保密和竞业禁止协议。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。

6.3.2 可信人员背景审查

背景审查包括对工作经历、职业推荐、教育、社会关系方面的审查，还可能包括对犯罪记录、档案、社会关系等方面的调查。

调查程序包括：

1)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。

2)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。

3)用人部门通过现场考核、日常观察、情景考验等方式对其考察。

4)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。

6.3.3 人员培训及再培训

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 E-GOV 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。

HNCA策略调整、系统更新时，组织员工进行再培训，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。

6.3.4 工作岗位轮换周期和顺序

HNCA根据岗位设置情况，结合人事部门具体规定，岗位要求相同或相近的岗位可按照人事具体规定定期进行岗位轮换。

6.3.5 违规行为处罚

HNCA 员工所有涉及到业务操作安全的操作均有记录，并定期进行审计。当发现员工涉嫌未授权行为、未授予的权力使用和对系统的未授权使用等，一经发现，HNCA 将立即中止该员工进入 HNCA 电子认证体系各系统。当事人的证书和操作权限即时冻结或注销，所做的未授权操作将立即被注销失效。同时，根据情节严重程度，对当事人作出相应处罚，包括内部处分、辞退、开除等，涉及犯罪的将送司法机关处理。

6.3.6 外包服务人员及要求

HNCA 的服务进行外包时，如果涉及敏感信息，应对外包服务商的安全服务能力进行评估，并由安全策略管理委员会审核批准。

HNCA 要求外包服务商对服务人员作出相应的安全承诺，并承担相应的安全责任。HNCA 严格限制外包服务人员所能接触的信息和权限，采取最小权限原则。

6.4 审计日志程序

6.4.1 审计日志定义

HNCA 按照安全要求，定期对安全事件进行审计，并记录审计日志。

6.4.2 审计日志安全检查与风险评估

HNCA 通过日志记录的事件进行安全检查与风险评估，主要包括：

- 密钥操作事件的审计。
- CA 系统操作或访问的事件审计。
- 网络安全相关事件的审计。
- 证书业务开展与业务规则的符合性审计。
- 敏感信息的访问审计。

6.4.3 审计日志记录要求

审计记录至少包括以下信息：

- 审计日期和事件。
- 审计的内容和意见。
- 审计操作的主体。
- 审计标识。

6.4.4 审计日志处理或归档周期

HNCA不定期对日志记录进行审查，经过审查并不存在异常的日志，可按要求进行归档。每年进行的审查不少于2次。

6.4.5 审计日志检测系统

对于CA系统、RA系统的安全事件记录由系统自动检查产生，保证非授权的访问能够被发现。

6.5 规定事件记录的类型

HNCA 规定记录的事件类型包括但不限于：

- 注册系统和证书受理操作的相关授权记录及管理记录；
- 密钥生成、备份、存储、撤销、归档和销毁管理；
- 密码设备生命周期管理；
- 证书申请、密钥更新、证书变更和证书撤销管理；
- 证书签发和 CRL 列表生成；
- PKI 系统访问；
- 操作 PKI 系统和其他安全系统的行为；
- 安全配置文件变更；
- 系统崩溃、硬件故障和其他异常；
- 防火墙和路由器的工作情况，机房进出访问。

6.6 规定事件记录的内容

每个事件的记录至少包括以下信息：

- 事件类型；
- 事件相关内容；
- 事件发生的时间日期；
- 数字签名审核程序时成功或失败的指示符；
- 证书撤销时成功或失败的指示符；
- 引起事件发生的实体或操作员身份。

6.7 记录归档要求

6.7.1 归档记录种类

HNCA 归档的记录包括审计日志和证书数据库文件、CA 密钥备份、HNCA 发行的证书、CRL、ARL、证书各种业务申请资料等。

6.7.2 记录归档的保存期限

HNCA 的记录归档保存期限至少为档案相关证书或密钥失效后 10 年。

6.7.3 记录归档的保护措施

HNCA 的记录归档保存在设有安全防护和防盗的物理环境中，并由专人管理，防止档案被修改、删除、非法取阅以及水、火、磁力、虫害等环境的损害。未经管理人员授权，任何人不得接近保存的档案。

6.7.4 记录归档的时间戳要求

HNCA 记录归档使用和业务系统相同的可靠时间源。

6.7.5 记录归档收集系统

HNCA 的记录归档系统分为人工处理和自动处理两部分组成。

6.7.6 记录归档验证机制

HNCA 在取阅档案信息时，需检查存储的档案是否存在删改和破坏现象，对于作了数字签名的档案，则需验证签名。

6.8 HNCA 的密钥更替

HNCA 使用国家根。国家根的密钥更替遵循国家根的有关规定。当发生以下情况时，为保障订户证书使用的安全性和合法性，HNCA 将立即申请进行密钥更替：

- 密钥对已经被泄漏、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；

- 国家相关主管机构对密钥算法、密钥长度等有变更规定。

HNCA 更替根密钥时采用与初始化根密钥相同的方式进行。更替过程中，原根密钥及信任链验证继续有效，确保不对现有应用造成影响。

6.9 数据备份

6.9.1 数据备份计划

HNCA 建立数据备份计划，由安全策略管理委员会明确具体的备份策略，备份内容至少应包括密钥、证书申请数据、证书数据、网络配置数据、CRL 数据。

6.9.2 异地备份中心

HNCA 采用同城异地备份机制，对用于 CA 系统恢复的相关软件、CA 密钥和日常的业务数据等进行备份，以便 CA 系统在受到灾难性毁灭时能够启动灾难恢复程序恢复服务。

6.10 损害与灾难恢复

6.10.1 事件和损害的列表

本章节所指事件和损害包括但不限于以下情况：

- HNCA 机房遭受物理损害，导致计算资源无法通过常规手段恢复。
- HNCA 核心业务系统当前使用的软件出现重大安全漏洞，经评估不能继续提供服务。
- HNCA 关键系统遭受攻击，经评估不能继续提供服务。
- HNCA 核心数据泄露或被破坏。
- 火灾或其他自然灾害。
- 其他不可抗力或不可预知的情况。

6.10.2 计算资源、软件或数据的损坏

当出现计算资源或软件或数据损坏，HNCA 启动安全事件的处理程序。评估事件的影响，防止事件扩大，并调查原因，利用备份机制重新建立安全环境，确

认事件影响范围，通过适当的方式通知受影响的订户，撤销或为其重新签发证书。必要时可能启动 CA 私钥损害处理或灾难恢复程序。

6.10.3 实体私钥损害处理程序

当 CA 私钥被攻破或泄露，HNCA 启动应急事件处理程序，由安全管理小组和相关的专家进行评估，制定行动计划。如果需要注销 CA 证书，会采取以下措施：

- 上报管理部门，并启动电子认证服务机构密钥更替流程；
- 发布证书注销状态到证书库；
- 在 HNCA 网站或其它通信方式发布关于注销 CA 证书的处理通报；
- 重新签发新的 CA 证书。

6.10.4 灾难后的业务连续性能力

HNCA为保证业务连续性，制定应急处理相关策略，定期进行演练并完善策略，确保其持续有效。

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，定期进行备机可用性检查，确保证书服务的高可靠性和可用性。

HNCA有异地数据备份，定期验证备份数据可用性，发生自然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。

6.11 CA 或 RA 业务终止

6.11.1 CA 业务终止

因各种原因，HNCA 计划暂停或终止电子认证业务情况下，HNCA 将按国家相关法律法规的要求进行业务终止操作。

HNCA 将努力寻找适合承接的认证机构，并在暂停或终止业务前六十个工作日前选择业务承接的认证机构，就业务承接有关事项通知有关各方，做出妥善安排，并在暂停或终止认证服务四十五个工作日前向国家密码管理局报告。不能就业务承接事项做出妥善安排的，将在暂停或终止业务前六十个工作日前，向国家密码管理局提出安排其它认证机构承接业务的申请。

无论如何，HNCA 继续按照本 E-GOV CPS 和国家法规的要求来处理档案和证书的续存工作。

6.11.2 注册机构业务终止

因各种原因，HNCA 所属注册机构计划暂停或终止证书业务情况下，注册机构应在暂停或终止业务前六十个工作日书面通知 HNCA，并通告其所办理证书的订户。HNCA 将作出妥善的安排，由其它注册机构或新设注册机构承接其业务，尽量减少对 CA 及证书订户的影响。

注册机构业务终止之日起 10 个工作日内，所有业务档案资料将无条件移交给 HNCA 或 HNCA 指定的承接注册机构。

7.认证系统技术安全控制规则

7.1 密钥对的生成和安装

7.1.1 密钥对的生成

HNCA 及其 RA、订户的所有密钥对，都是由国家密码主管部门许可使用的密码设备或模块生成。HNCA 根密钥对及其下级 CA 密钥对的生成，是在预设定的程序下，由至少 3 名密钥管理员及 1 名监督人员参与下产生，并对每个环节进行记录和签名。订户的签名密钥对由其持有的电子密匙或其它密码设备产生，而加密密钥对由河南省国家密码管理局的密钥管理基础设施产生。

7.1.2 私钥的传递

HNCA 的私钥只能保存在 HNCA 控制的密码设备和采取秘密分割的备份介质中，禁止向外传递。

订户的签名私钥在订户的电子密匙中直接生成，或其它密码设备生成后随其实物通过离线方式传递到订户；而订户的加密私钥在 KMC 产生后，使用订户对应电子密匙或其它密码设备预生成的公钥加密后经过 CA、RA 传递回订户对应的电子密匙或其它密码设备中，HNCA 可使用 SSL 会话等方式传递私钥以保证安全性。

电子密匙或其它密码设备的离线传递，可以是 CA 或 RA 和订户面对面的交递，或采取密码信封保护方式发送（如邮递）给订户。

7.1.3 公钥传递给签发机构

订户的公钥采用证书签发请求格式（PKCS#10）或其它约定的安全格式通过安全通道传递给 HNCA，由 HNCA 完成证书签发。

7.1.4 认证机构公钥传递给依赖方

HNCA 的公钥随 HNCA 根证书发布到 HNCA 信息库供订户和依赖方下载。

7.1.5 密钥的算法

HNCA 使用的密钥算法均为国家密码管理局认可的算法。

7.1.6 公钥参数的生成和质量检查

HNCA 负责生成密钥时，公钥参数由国家密码主管部门许可的设备或模块产生，HNCA 不会专门安排其质量检查。

7.1.7 密钥使用目的

在 HNCA 认证体系中的密钥用途和证书类型紧密相关，分为签名和加密两大类。

HNCA 的签名密钥可用于签发下级 CA、订户证书和 CRL。

RA 的签名密钥用于确认 RA 所做的审核证书等操作。

订户的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、接收方能够通过数字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。订户的加密密钥用于对需在网络上传送的信息进行加密，保证信息除发送方和接受方外不被其他人窃取、篡改。

更多与协议和应用相关的密钥使用限制请参阅 X.509 标准中的密钥用途扩展域。

7.2 私钥保护与密码模块工程控制

7.2.1 密码模块标准与控制

HNCA 使用国家密码主管部门许可的密码产品，其密码模块符合国家规定的标准要求。

7.2.2 在 CA 私钥保护方面的要求

HNCA 采用多人控制策略来管理（包括生成、激活、备份、恢复、停止、销毁）CA 的私钥。HNCA 使用国家密码主管部门许可的硬件密码设备来生成和保护 CA 的私钥。通过密码设备支持的 N 选 M（其中 N 至少为 5，M 至少为 3 但不大于 N）方式进行私钥的分割，即将管理私钥的数据分割成 N 个部分，由密钥管理人员分别持有，并至少需要 M 个“秘密分享”持有者参与才能实现私钥的管理。

7.2.3 订户私钥保护方面的要求

订户的签名密钥对由订户掌握的密码设备生成和管理，为订户专有。

订户的加密密钥对由国家密码管理局和省级密码管理部门规划建设的密钥管理基础设施提供密钥管理服务。

7.3 密钥对管理的其他方面

7.3.1 公钥归档

HNCA 和 HNCA 订户的公钥会随其证书作为 HNCA 安全运行数据被存放或被归档在目录服务器或数据库中，并在其失效后仍会在 HNCA 系统中保存至少 10 年。

7.3.2 证书操作期和密钥对使用期限

1）公钥和私钥的使用期限与证书的有效期相关但却有所不同。

2）对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期限以外。

3）对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

4）对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

5）当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

7.4 激活数据

7.4.1 激活数据的产生和安装

激活数据指用于激活私钥的口令、PIN 码或“秘密分享”数据等。

HNCA 的“秘密分享”数据由硬件加密模块产生（参见本文 7.2.2），符合相应安全要求。

7.4.2 激活数据的保护

HNCA 私钥的激活数据由采用“秘密分享”的办法由不同的可信人员管理（参见本文 7.2.2）。

如果证书持有者使用口令或 PIN 码保护私钥，证书持有者应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书持有者使用生物特征保护私钥，证书持有者也应注意防止其生物特征被人非法获取。

7.4.3 激活数据的其他方面

- 激活数据的传送

当私钥的激活数据进行传送时，应保护它们在传送过程中免于丢失、偷窃、修改、非授权泄露或非授权使用。Windows 或网络的登录用户的用户名/密码（用于证书持有者激活数据），经过网络传送时注意非法用户的窃取。

- 激活数据的销毁

当私钥的激活数据不需要时应该销毁，并保护它们在此过程中免于丢失、偷窃、泄露或非授权使用，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或全部，比如记录有口令的纸张必须粉碎。

7.5 系统安全控制

7.5.1 安全技术要求

HNCA 用于运行认证系统和处理数据的生产用的系统安全可信，不会受到未经授权的访问，HNCA 只允许有工作需求的人员经过授权后访问认证系统服务器。

7.5.2 安全技术措施

HNCA 的生产系统网络采用多级不同厂家的防火墙逻辑隔离各安全区域，并部署有入侵检测系统。HNCA 计算机的管理员账号口令必须符合复杂度要求，并定期更改这些口令。

7.6 生命周期技术控制

7.6.1CA 系统运行管理

制定 CA 系统的操作流程并及时维护。

HNCA 对认证系统生命周期内的任何补丁和升级版本进行控制，并只有授权的人员才能访问。任何对认证系统安全性有影响的改动须先进行风险评估，并由安全管理小组批准。

HNCA 采取检测和防护手段来保证系统运行环境的安全，并能提供适当的报警信息。建立系统事件处理流程，确保发现的任何异常情况能有效处理。

制定介质管理制度，对相关介质进行妥善管理，避免非授权的访问。

7.6.2CA 系统访问管理

明确 CA 系统的访问策略、相关角色权限及鉴别方法，定义角色职能，合理分割权限，制定授权流程和策略。

制定网络和操作系统安全策略、访问策略。建立审计制度。

7.6.3CA 系统开发和维护

HNCA 的认证系统由商用密码产品生产定点单位研制，符合国家的相关标准和规范。HNCA 要求其内部或外包的软件开发项目符合 ISO9001:2008 质量要求，

并遵守国家的法规和签署的项目保密条款。HNCA 的认证系统首次部署后经国家密码主管部门组织的专家组进行技术鉴定后启用。

严格控制对 CA 系统源码及测试数据的访问权限。建立 CA 版本控制，对系统的新增或修改进行管理。

7.7 网络的安全控制

HNCA 认证系统根据信息敏感度的不同，划分为不同的区域，每个区域之间配备不同厂家的异构防火墙进行保护，并配置入侵检测系统，与防火墙联动。CA 与 RA 的功能模块之间的通信采用 VPN 或其它安全通信协议连接，并采用安全身份认证技术。

HNCA 对网络安全设备的软件版本、规则及时更新，保持其有效的工作状态。只有系统管理员或专门授权人员才能管理这些网络设备。并且这些设备的管理员账号口令有最小密码长度和复杂度要求，系统管理员定期更改这些口令。

7.8 时间戳

HNCA 电子认证服务系统使用统一的内部时间源服务，保证系统日志记录时间的准确性和一致性。

8.法律责任和其它业务条款

8.1 费用

8.1.1 免费或收费策略

HNCA根据市场情况和提供的电子认证服务内容确定价格政策，并可在HNCA网站上予以公布。

HNCA根据市场情况和订户享有的服务内容确定收费标准。订户有义务根据HNCA与之确定的价格向HNCA支付费用。

如果HNCA签署的协议中指明的收费标准和HNCA公布的价格不一致时，以协议中的收费标准为准。

8.1.2 证书签发和更新费用

HNCA收取合理的证书签发和更新费用，并在用户订购时提前告知。

8.1.3 证书查询费用

通过HNCA信息库进行证书查询，目前不收取任何费用。

8.1.4 证书撤销或状态信息查询费用

通过HNCA信息库进行对证书撤销或状态信息查询，目前不收取任何费用。

8.1.5 其它服务费用

HNCA保留收取其他服务费的权利。

8.1.6 退款政策

在实施证书操作和签发证书的过程中，HNCA遵守并保持严格的操作程序和策略。一旦订户接受证书，HNCA将不办理退证、退款手续。

如果订户在证书服务期内退出证书服务体系，HNCA将不退还剩余时间的服务费用。

8.2 财务责任

8.2.1 责任担保范围

HNCA 根据业务发展情况决定其担保范围，目前暂无。

8.2.2 责任赔付声明

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。

8.3 业务信息保密

8.3.1 保密信息范围

HNCA 列入保密的信息包括但不限于以下内容：

- 订户的个人信息和（或）机构信息；
- HNCA 及其代理机构的证书业务处理信息；
- 所有的私钥信息；
- HNCA 的运行数据和记录，以及保障运行的相关计划；
- HNCA 与业务代理机构间的商业信息，包括商业计划、销售信息、贸易秘密和公开协议下从第三方得到的信息；
- HNCA 及其业务代理机构相关的审计报告、审计结果及其处理等信息；
- 除非法律明文规定，HNCA 没有义务公布或透露订户证书以外的任何信息；
- 其它书面或有形形式确认为保密的信息。

8.3.2 不在保密范畴内的信息

以下信息 HNCA 不列入保密范畴：

- 证书所载信息，以及证书状态信息；
- 由 HNCA 网站或手册公布的信息。包括证书申请流程、证书使用指南、E-GOV CPS、CRL 等信息。

以上信息虽然是公开信息，但仅供下载查阅使用，任何人或组织不得转载或用于任何商业用途，HNCA 保留追究责任的权利。

8.3.3 保护保密信息的责任

HNCA 及其业务代理机构、订户、关联实体等所有保密信息掌握者均有义务承担信息保密的责任。

HNCA 执行严格的信息保密制度以确保只有经 HNCA 授权的人员才能接触机密信息。严格禁止未授权的访问、阅读、修改和删除等操作。

当机密信息的所有者出于某种原因，要求 HNCA 公开或披露其所拥有的机密信息，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

果这种披露机密的行为涉及任何其他方的赔偿义务，HNCA 不应承担任何与此相关的或由于公开机密信息引起的所有损失、损坏的赔偿责任。

当 HNCA 在国家的法律法规要求下，或在法院的要求下必须披露本文 8.3.1 中的保密信息时，HNCA 可以按照法律法规或法院判决的要求，向执法部门公布相关的保密信息。这种披露不能视为违反了保密的要求和义务，HNCA 无须承担任何责任。

8.4 个人隐私保密

8.4.1 保护隐私信息的责任

HNCA 对开展业务过程中所接收的属于私有信息的个人隐私信息进行保护，防止泄露。只有经 HNCA 授权的人员才能接触隐私信息，禁止任何未授权的访问、阅读或转移。

8.4.2 使用隐私信息的告知与同意

HNCA 只在其业务范围内使用订户隐私信息，包括订户身份识别、管理和服务的目的。这些使用，HNCA 没有告知订户的义务，也无需得到订户的同意。

任何超出以上范围的隐私信息使用，需得到其本人的同意。对违法、违规使用、发布以上隐私信息的，HNCA 承担由此造成的证书持有者、依赖方的损失，并承担相应的行政、经济责任。

8.4.3 依法律或行政程序的信息披露

当 HNCA 在国家的法律、规章的要求下，或在法院的要求下必须披露订户隐私信息时，HNCA 可以按照法律、规章或法院判决的要求，向执法部门公布相关的隐私信息。这种披露不能视为违反了保密的要求和义务，HNCA 无须承担任何责任。

8.4.4 其他信息披露情形

当订户出于某种原因，要求 HNCA 公开或披露他的隐私信息，HNCA 可根据授权或协议进行披露。如果这种披露行为涉及任何其他方的赔偿义务，HNCA 不承担任何与此相关的或由于公开隐私信息引起的所有损失、损坏的赔偿责任。

8.4.5 不被视为隐私的信息

所有在证书、CRL 载明的订户信息不被视为隐私信息。

8.5 知识产权

8.5.1 HNCA 自身拥有的知识产权声明

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，包括但不限于所有权、名称权和利益分享权等。

HNCA 发行的证书及其状态信息，以及 HNCA 提供的软件、系统、文档中，使用、体现和涉及到的一切版权、商标和其他知识产权均属于 HNCA，这些知识产权包括所有相关的文件、E-GOV CPS、规范文档和使用手册等。

在没有 HNCA 预先书面同意的情况下，订户不能在任何证书到期、作废或终止的期间或之后，使用或接受任何 HNCA 使用的名称、商标、交易形式或可能与之相混淆的名称、商标、交易形式或商务称号。

8.5.2 HNCA 使用其他方知识产权的声明

订户或证书申请者声明并保证其交付给 HNCA 使用的网络域名、IP 地址、主体名称及所有其它证书申请书的资料不得在任何管辖区域内干预或侵犯第三人的商标、服务标志、公司名称或其它知识产权等权利，而且不用于非法目的，包括侵害、干扰协议或预期的商业利益、不公平竞争、损害他人信誉及干扰或误导他人。

8.6 陈述与担保

8.6.1 HNCA 的陈述与担保

HNCA 的担保如下：

- HNCA 遵守《中华人民共和国电子签名法》及相关法律的规定，接受国家密码管理局的监管，对签发的数字证书承担相应的法律责任。
- 在批准证书申请和颁发证书中没有 HNCA 所知的或源自 HNCA 的错误陈述。

- 在生成证书时，保证足够检测和审核，使证书中的信息与 HNCA 所收到的信息保持一致。
- 证书中的或证书中合并参考到的所有信息都是准确的。
- 签发给订户的证书符合本 E-GOV CPS 的所有实质性要求。
- HNCA 将向订户和依赖方通报任何已知的，将在根本上影响证书的有效性和可靠性的事件。
- 其它的陈述与担保参见与订户的服务协议。

8.6.2 RA 的陈述与担保

HNCA 的 RA 担保如下：

- RA 遵循 HNCA 制订的服务受理规范、系统运作和管理要求，保证其服务不影响到 HNCA 的服务标准和承诺。
- 在审核和批准证书申请中没有 RA 所知的或源自 RA 的错误陈述。
- 在处理证书申请时，保证足够检测和审核，使证书中的信息与 RA 所收到的信息保持一致。
- 证书中的或证书中合并参考到的所有信息都是准确的。
- 签发给订户的证书符合本 E-GOV CPS 的所有实质性要求。
- 按本 E-GOV CPS 的规定，及时处理证书的注销申请。
- 其它的陈述与担保参见与订户的服务协议。

8.6.3 订户的陈述与担保

订户的担保如下：

- 用与证书中所含公钥相对应的私钥所进行的每一次签名，都是订户自己的签名，并且在进行签名时，证书是有效的（没有过期或注销）并已被订户接受。
- 订户的私钥得到很好的保护，未经授权的人员从未访问过其私钥。
- 订户在证书申请过程中 HNCA 及其 RA 陈述的所有信息是真实的。
- 订户提供给 HNCA 及其 RA 用于申请证书的所有材料都是真实的。
- 如果存在代理人，那么订户和代理人两者负有连带责任。订户有责任就代理人所作的任何不实陈述与遗漏，通知 HNCA 其 RA。

- 订户将按本 E-GOV CPS 的规定，只将证书用于经过授权的、合法的使用目的。
- 订户的证书是终端证书。订户保证不将其证书用于发证机构所从事的业务，例如：把与证书中所含的公钥所对应的私钥用于签发任何证书（或认证其他任何形式的公钥）或签发 CRL 之类。
- 其它的陈述与担保参见与 HNCA 的服务协议。

8.6.4 依赖方的陈述和担保

依赖方的担保如下：

- 依赖方保证熟悉 HNCA E-GOV CPS 以及和订户证书相关的证书政策，并了解和遵守证书的使用目的。依赖方确保证书及其对应的密钥对的确用于预定的目的。
- 依赖方在信赖订户的证书前，需收集足够的信息，判明是否 HNCA 签发的证书并在有效期内，根据最新的 CRL 检查证书的状态，查明证书是否还有效。
- 依赖方的信赖行为，表明其已同意本 E-GOV CPS 的有关条款。

8.7 担保免责

HNCA 在以下三种情况下免除责任：

1）不可抗力。在不可抗力情况下（内容见本文 8.16.5 和相关法律条款），HNCA 免除责任。

2）免责条款

免责条款是指当事人在合同中约定的免除将来可能发生的违约责任的条款。免责条款不得违反法律的强制性规定和社会公共利益。

3）债权人过错

如果合约不履行或者不完全履行是由对方即债权人的过错造成的，不履行或者不完全履行的一方免除违约责任。在电子认证服务合同中也存在因债权人过错而免责的情况，包括但不限于以下内容：

- 申请者故意或无意的提供不完整、不可靠或已过期的，包括但不限于伪造、篡改、虚假的信息，而其又根据正常的流程提供了必须的审核文件，由此得到了 HNCA 签发的数字证书。

- 订户或依赖方没有使用可信赖系统进行证书操作。
- 订户在 HNCA 允许的目的范围之外使用或证书使用不当。

以上未尽事宜，依照中华人民共和国现行法律、法规执行。

8.8 HNCA 偿付责任限制

HNCA是依《中华人民共和国公司法》、《中华人民共和国电子签名法》设立的有限责任公司，HNCA 在承担任何责任和义务时，只承担法律范围内的有限责任。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。

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：

1)证书信息与订户提交的信息资料不一致，造成订户损失。

2)因HNCA原因，致使订户证书无法正常使用，造成订户损失。

3)HNCA只在证书有效期限内承担损失或损害赔偿。

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。

8.9 订户和依赖方责任

订户和依赖方在使用和信赖证书时，如有任何行为或疏忽导致 HNCA 或其他方产生损失，则订户或依赖方应承担赔偿责任。

8.9.1 订户的赔偿责任情况

- 订户申请证书时，因故意、过失或者恶意提供不真实资料，造成 HNCA 或者其他方遭受损害的。
- 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知 HNCA 或其 RA，以及使用不安全系统或不当交付他人使用，造成 HNCA 或其他方遭受损害的。
- 订户提供使用的命名信息，包括但不限于名称、域名、IP、电子邮箱等，存在任何侵犯他人知识产权，造成 NETCA 或其他方遭受损害的。

8.9.2 依赖方的赔偿责任情况

- 未按 HNCA E-GOV CPS 或其他相关协议承担依赖方义务，而造成 HNCA 或其他方遭受损害的。
- 未能按 HNCA E-GOV CPS 策略识别和信任证书及其行为，而造成 HNCA 或其他方遭受损害的。
- 未查验证书的有效期和状态就贸然信任证书及其行为，而造成 HNCA 或其他方遭受损害的。

8.10 有效期限与终止

8.10.1 有效期限

HNCA E-GOV CPS 自发布之日起正式生效。E-GOV CPS 中将详细注明版本号及发布日期。

8.10.2 终止

当新版本的 E-GOV CPS 正式发布生效时，旧版本的 E-GOV CPS 将自动终止。

HNCA 通过 HNCA 网站或符合规定的其他途径声明 E-GOV CPS 终止。

8.10.3 效力的终止与保留

HNCA E-GOV CPS 一旦终止后，订户和依赖方原则上不受其条款的约束，但涉及知识产权和保密的相关条款继续生效。

8.11 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。

8.12 修订

8.12.1 修订程序

当E-GOV CPS不适用时，由HNCA安全策略管理委员会委托执行组对E-GOV CPS进行修订。安全策略管理执行组负责起草新的E-GOV 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E-GOV CPS文本格式和版本号，形成定稿，报总经理审批；总经理审批同意后，方可对外发布，并报送国家密码管理局备案。

8.12.2 通告机制和期限

本E-GOVCPS在HNCA网站上发布。

版本更新时，最新版本的E-GOV CPS在HNCA网站发布，对具体个人不做另行通知。

8.12.3 必须修改 E-GOV CPS 的情形

如果出现下列情况，那么必须对 E-GOV CPS 进行修改：

- 采用了新的密码体系或技术，并影响现有 E-GOV CPS 的有效性。
- 认证系统和有关管理规范发生重大升级或改变。
- 法律法规的变化，并影响现有 E-GOV CPS 的有效性。
- 现有 E-GOV CPS 出现重要缺陷。

8.13 争议处理

如果 HNCA 与合作机构之间或与订户、依赖方之间发生争议，而当事人之间无法很好的解决出现的问题和争端，均提请郑州仲裁委员会按照该会仲裁规则进行仲裁。仲裁裁决是终局的，对双方均具有约束力。

证书订户、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，根据本 E-GOV CPS 中的规定，明确责任方；

2)由相关部门负责与当事人协调；

3)若协调失败，可以通过司法途径解决；

4)任何因与 HNCA 或授权机构就本 E-GOV 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。

8.14 管辖法律

HNCA E-GOV CPS 在各方面按照中国现行法律和法规执行和解释。包括但不限于《中华人民共和国电子签名法》及《电子政务电子认证服务管理办法》、《电子认证服务密码管理办法》等。

8.15 与适用法律的符合性

HNCA 电子认证业务各参与方必须遵守中国现行法律及相关行业规范的监管，包括但不限于《中华人民共和国电子签名法》、《中华人民共和国网络安全法》、《商用密码管理条例》、《电子政务电子认证服务管理办法》、《电子认证服务密码管理办法》及国家密码管理局相关密码技术、产品标准规范等。

8.16 一般条款

8.16.1 完整协议条款

HNCA E-GOV CPS 及 HNCA 的相关业务管理办法、国家相关法律法规构成 HNCA 的整体协议，各参与方的业务须遵循整体协议。

8.16.2 转让条款

若 HNCA 下属 RA 因故注销，则其管理的相应订户须接受 HNCA 的业务调配，通过另一 RA 获得相应服务;若 HNCA 因政策性原因或其它不可抗力停止服务,HNCA 所属订户须按国家规定，接受相应接管 CA 的证书服务条款。

8.16.3 分割性条款

在 HNCA 的电子认证业务中，因某一原因导致法庭或其它仲裁机构判定协议中的某一条款无效或不具执行力时（由于某种原因），订户证书业务相关协议的其它条款仍然生效。

8.16.4 强制执行条款

HNCA 电子认证各参与方中，免除一方对合约某一条款违反应负的责任，不意味着免除这一方对其它条款违反或继续免除这一方对该条款违反应负的责任。

8.16.5 不可抗力条款

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；如战争、罢工、骚乱、恐怖活动等社会异常事件。

在电子认证活动中，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，也可根据不可抗力的影响而部分或者全部免除违约责任。其他认证活动参与各方（如订户）不得就此提出异议或者申请任何补偿。

由于法律无法具体规定或者列举不可抗力的内容和种类,加上不可抗力本身的弹性较大，在理解上容易产生歧义，因而允许当事人在合同中订立不可抗力条款，根据交易的情况约定不可抗力的内容和种类。HNCA 电子认证合同中的不可抗力条款可以在与数字证书申请表一起提供给订户的服务协议中规定,也可被规定在 HNCA E-GOV CPS 中。

8.17 其它条款

8.17.1 各种规定的冲突

若 HNCA E-GOV CPS 的规定与其它规定、指导方针或协议相互抵触，各参与方必须接受 HNCA E-GOV CPS 的约束，除非:

- HNCA E-GOV CPS 的规定为法律所禁止范围内；
- 该冲突的协议签署日期在 HNCA E-GOV CPS 首次公开发行之前；
- 该冲突的协议明确优于 HNCA E-GOV CPS。

8.17.2 安全资料的财产权益

除非另有约定，下列与安全相关的资料视为下列指定的当事人所拥有：

- 证书：证书为 HNCA 的产权所有。
- HNCA E-GOV CPS：HNCA E-GOV CPS 的版权为 HNCA 所有。
- 甄别名：甄别名为该命名实体（或其雇主或委托人）所有。
- 私钥：不论该密钥是以何种实体媒介存放或保护，私钥为合法使用或有权使用该密钥订户（或其雇主或委托人）所有。
- 公钥：不论该密钥以何种实体媒介存放或保护，公钥为订户（或其雇主或委托人）所有。
- HNCA 的私钥：HNCA 的私钥是 HNCA 的财产。这些私钥由 HNCA 授权分配和使用。
- HNCA 的公钥：HNCA 的公钥是 HNCA 的财产。HNCA 允许使用这些公钥。

8.17.3 损害性资料

证书申请者与订户不能把包含以下言论的任何资料提交给 HNCA 或其 RA：

- 毁谤、中伤、不雅、色情、侮辱、迷信、憎恶或种族歧视的言论；
- 鼓吹非法活动或讨论非法活动，并试图从事此类活动的言论；
- 其它违法言论。