HNCA电子政务电子认证服务业务规则

(版本3.0)

(生效日期：2017年6月1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

目 录

1.概括性描述 10
1.1 概述 10
1.2 文档名称 10
1.3 电子认证活动参与方及其职责 10
1.3.1 电子认证服务机构 10
1.3.2 注册机构 11
1.3.3 订户 11
1.3.4 依赖方 12
1.3.5 其他参与者 12
1.4 证书应用 12
1.4.1 适合的证书应用 12
1.4.2 证书订户性质 13
1.4.3 限制的证书应用 13
1.5 策略管理 13
1.5.1 策略文档管理机构 13
1.5.2 联系信息 14
1.5.3 决定 E-GOV CPS 符合策略的机构 14
1.5.4 E-GOV CPS 批准程序 14
1.6 定义和缩写 14
2.信息发布与信息管理 16
2.1 信息库 16
2.2 认证信息的发布 17
2.2.1 E-GOV CPS 的发布 17
2.2.2 证书和 CRL 发布 17
2.3 发布时间或频率 18
2.3.1 E-GOV CPS 的发布时间或频率 18
2.3.2 证书的发布时间或频率 18
2.3.3 CRL 的发布时间或频率 18
2.4 信息库访问控制 18
3.身份标识与鉴别 19
3.1 命名 19
3.1.1 DN 说明条款 19
3.1.2 名称类型 20
3.1.3 订户的匿名或伪名 20
3.1.4 名称的唯一性 20
3.2 初始身份确认 20
3.2.1 证明持有私钥的方法 20
3.2.2 机构身份的鉴别 20
3.2.3 个人身份的鉴别 21
3.2.4 不予验证的订户信息 21
3.2.5 授权确认 22
3.2.6 审核认证体系成员身份确认 22

3.2.7 互操作准则 22
3.3 密钥更新请求的身份鉴别 22
3.4 证书吊销请求的身份鉴别 23
4.证书生命周期操作要求 23
4.1 证书申请 23
4.1.1 证书申请实体 23
4.1.2 申请过程与责任 23
4.2 证书申请处理 24
4.2.1 身份审核 24
4.2.2 证书申请批准和拒绝 24
4.2.3 处理证书申请的时间 24
4.3 证书签发 25
4.3.1 证书签发过程 25
4.3.2 电子认证服务机构对订户的通告 25
4.4 证书接受 25
4.4.1 构成接受证书的方式 25
4.4.2 电子认证服务机构对证书的发布 25
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 26
4.5 密钥对和证书的使用 26
4.5.1 订户私钥和证书的使用 26
4.5.2 依赖方对公钥和证书的使用 26
4.6 证书更新 27
4.6.1 证书更新的情形 27
4.6.2 证书更新请求的处理 27
4.6.3 颁发新证书时对订户的通告 27
4.6.4 构成接受更新证书的行为 27
4.6.5 电子认证服务机构对更新证书的发布 27
4.7 证书密钥更新 28
4.7.1 证书密钥更新的情形 28
4.7.2 证书密钥更新请求的处理 28
4.7.3 颁发新证书对订户的通告 28
4.7.4 构成接受密钥更新证书的行为 28
4.7.5 电子认证服务机构对密钥更新证书的发布 28
4.8 证书变更 28
4.8.1 证书变更的情形 29
4.8.2 证书变更请求的处理 29
4.8.3 颁发新证书时对订户的通告 29
4.8.4 构成接受变更证书的行为 29
4.8.5 电子认证服务机构对变更证书的发布 29
4.9 证书吊销 29
4.9.1 证书吊销的情形 29
4.9.2 吊销请求的处理 30
4.9.3 吊销请求宽限期 30
4.9.4 证书挂起 31

4.9.5 证书吊销状态的发布 31
4.9.6 依赖方检查证书状态的要求 31
4.10 证书状态服务 31
4.10.1 操作特点 31
4.10.2 服务可用性 31
4.10.3 可选特征 31
4.11 订购结束 32
4.12 密钥生成、备份与恢复 32
4.12.1 密钥生成和备份 32
4.12.2 密钥的恢复 32
4.12.3 密钥对的存储和恢复安全策略 33
4.12.4 会话密钥的封装与恢复的策略和行为 33
5.认证机构设施管理和操作控制 33
5.1 物理控制 33
5.1.1 机房的建筑 33
5.1.2 物理访问 33
5.1.3 电源和空调 34
5.1.4 水患防治 34
5.1.5 火灾预防和保护 34
5.1.6 介质存储 34
5.1.7 废物处理 35
5.1.8 异地备份 35
5.1.9 入侵红外报警系统 35
5.2 操作过程控制 35
5.2.1 可信角色 35
5.2.2 角色要求的人数 36
5.2.3 可信角色的鉴别 36
5.2.4 职责需分离的角色 36
5.3 人员控制 37
5.3.1 人员资格要求 37
5.3.2 背景调查程序 37
5.3.3 培训要求 37
5.3.4 再培训要求 38
5.3.5 对未授权操作的处理 38
5.4 审计日志程序 38
5.4.1 记录事件的类型 38
5.4.2 日志的处理周期 39
5.4.3 审计日志的保存期限 39
5.4.4 审计日志的保护 39
5.4.5 审计日志的备份 39
5.4.6 审计日志的采集 40
5.4.7 对导致事件实体的通告 40
5.4.8 脆弱性评估 40
5.5 记录归档 40

5.5.1 归档记录种类 40
5.5.2 档案保存期限 40
5.5.3 档案的保护 40
5.5.4 档案备份 40
5.5.5 档案的标识 41
5.5.6 档案采集系统 41
5.5.7 档案验证 41
5.6 CA 的密钥更替 41
5.7 损害和灾难恢复 41
5.7.1 HNCA 遭攻击或发生损害事故时的恢复程序 41
5.7.2 计算资源、软件或数据的破坏处理 42
5.7.3 CA 私钥损害的处理 42
5.7.4 灾难发生后的业务保持 42
5.8 CA 或 RA 业务终止 42
5.8.1 CA 业务终止 42
5.8.2 注册机构业务终止 43
6.认证系统技术安全控制 43
6.1 密钥对的生成和安装 43
6.1.1 密钥对的生成 43
6.1.2 私钥的传递 43
6.1.3 公钥的传递 44
6.1.4 密钥长度 44
6.1.5 公钥参数的产生 44
6.1.6 密钥用途 44
6.2 私钥保护与密码模块的控制 45
6.2.1 密码模块标准与控制 45
6.2.2 私钥的分割管理 45
6.2.3 私钥托管 45
6.2.4 私钥备份 45
6.2.5 私钥归档 45
6.2.6 私钥在密码模块中的导入和导出 46
6.2.7 私钥在密码模块中的保存 46
6.2.8 私钥的激活 46
6.2.9 私钥的停止 46
6.2.10 私钥的销毁 46
6.3 密钥对的其它管理 47
6.3.1 公钥归档 47
6.3.2 密钥对与证书的有效期 47
6.4 激活数据 47
6.4.1 激活数据的产生 47
6.4.2 激活数据的保护 47
6.5 计算机安全控制 48
6.5.1 计算机安全性要求 48
6.5.2 计算机安全评估 48

6.6 生命周期技术控制 48
6.6.1 系统开发控制 48
6.6.2 系统改进控制 48
6.6.3 安全管理控制 49
6.7 网络安全性控制 49
6.8 时间戳 49
7.证书、CRL 和发布服务 49
7.1 证书 49
7.1.1 版本号 49
7.1.2 证书扩展项 49
7.1.3 算法 OID 50
7.1.4 名称形式 51
7.1.5 证书密钥用法 51
7.2 CRL 52
7.2.1 版本号 52
7.2.2CRL 和 CRL 条目扩展项 52
7.3 发布服务 52
7.3.1 版本号 52
7.3.2 OCSP 扩展项 52
8.认证机构审计和其他评估 52
8.1 审计的依据 53
8.2 审计的形式 53
8.3 审计或评估的频率 53
8.4 审计或评估人员的资质 53
8.5 审计或评估人员与 HNCA 的关系 53
8.6 审计或评估的内容 54
8.7 对问题与不足采取的措施 54
8.8 审计或评估结果的传达与发布 54
9.法律责任和其它业务条款 54
9.1 费用 54
9.1.1 证书签发和更新费用 55
9.1.2 证书查询费用 55
9.1.3 证书吊销或状态信息查询费用 55
9.1.4 其它服务费用 55
9.1.5 退款政策 55
9.2 财务责任 55
9.3 业务信息保密 55
9.3.1 保密信息的范围 55
9.3.2 不在保密范畴内的信息 56
9.3.3 保护保密信息的责任 56
9.4 个人隐私保密 57
9.4.1 隐私保护方案 57
9.4.2 作为隐私处理的信息 57
9.4.3 不被视为隐私的信息 57

9.4.4 保护隐私信息的责任 57
9.4.5 使用隐私信息的告知与同意 57
9.4.6 依法律或行政程序的信息披露 57
9.4.7 其他信息披露情形 58
9.5 知识产权 58
9.5.1 HNCA 自身拥有的知识产权声明 58
9.5.2 HNCA 使用其他方知识产权的声明 58
9.6 陈述与担保 59
9.6.1 HNCA 的陈述与担保 59
9.6.2 RA 的陈述与担保 59
9.6.3 订户的陈述与担保 60
9.6.4 依赖方的陈述和担保 60
9.7 担保免责 60
9.8 HNCA 偿付责任限制 61
9.9 订户和依赖方责任 62
9.9.1 订户的赔偿责任情况 62
9.9.2 依赖方的赔偿责任情况 62
9.10 有效期限与终止 63
9.10.1 有效期限 63
9.10.2 终止 63
9.10.3 效力的终止与保留 63
9.11 对参与者的个别通告与沟通 63
9.12 修订 63
9.12.1 修订程序 63
9.12.2 通告机制和期限 64
9.12.3 必须修改 E-GOV CPS 的情形 64
9.13 争议处理 64
9.14 管辖法律 64
9.15 与适用法律的符合性 65
9.16 一般条款 65
9.16.1 完整协议条款 65
9.16.2 转让条款 65
9.16.3 分割性条款 65
9.16.4 强制执行条款 65
9.16.5 不可抗力条款 65
9.17 其它条款 66
9.17.1 各种规定的冲突 66
9.17.2 安全资料的财产权益 66
9.17.3 损害性资料 67
10.支持服务管理 67
10.1 服务内容 67
10.1.1 面向证书持有者订户的服务支持 67
10.1.2 面向应用提供方的服务支持 67
10.2 服务方式 68

10.2.1 坐席服务 68
10.2.2 在线服务 68
10.2.3 现场服务 68
10.2.4 满意度调查 68
10.2.5 投诉处理 68
10.2.6 培训 69
10.3 服务质量 69
10.4 证书应用集成支持服务 69
10.4.1 证书应用集成内容 69
10.4.2 证书应用接口 70
10.4.3 证书应用集成服务 70
10.4.4 决策支持信息服务 70

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。

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 文档名称

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发布的第三个版本，版本号V3.0。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。

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

电子认证服务机构是受订户信任，负责创建和分配公钥证书的权威机构，是颁发数字证书的实体。HNCA设立策略管理委员会、执行小组等机构，进行相关管理活动。HNCA下设运营中心及业务受理点，进行业务管理及实施活动。

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

国家RSA2048算法根证书的DN为：

CN = ROOTCA

O = OSCCA

C = CN

国家根为HNCA签发的RSA2048根证书DN为：

CN = HNCA

O = HENAN CERTIFICATE AUTHORITY

L = ZZ

S = HN

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。

1.4 证书应用

1.4.1 适合的证书应用

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http://www.hnca.com.cn和http://www.9611111.com上的介绍，证书申请人根据实际需要，决定采用哪种证书类型。

1.4.2 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

1.4.3 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。

1.5 策略管理

1.5.1 策略文档管理机构

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

HNCA E-GOV CPS由HNCA拥有完全版权。

1.5.2 联系信息

HNCA E-GOV CPS在HNCA网站发布，对具体个人不另行通知。

网站地址：http://www.hnca.com.cn和http://www.9611111.com；

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：0371-68107818；

传真号码：0371-68107808。

1.5.3 决定 E-GOV CPS 符合策略的机构

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

1.5.4E-GOV CPS 批准程序

策略管理委员会执行小组负责起草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策略管理委员会审阅；执行小组依据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。

HNCA E-GOV CPS 从对外公布之日起三十日之内向国家密码管理局备案。

1.6 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人，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)电子签名认证证书(证书)Digital Certificate

是电子认证服务提供者签发的用以证明证书持有人的电子签名、身份、资格及其他有关信息的电子文件。证书包含有公开密钥拥有者的信息、公开密钥、签名算法和CA的数字签名。

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)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。

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。

2.信息发布与信息管理

2.1 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、证书服务协议、技术支持手册和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的网站上（http://www.hnca.com.cn和http://www.9611111.com)。信息库将及时发布包括证书、

E-GOV CPS 修订、证书注销的通知和其它资料等内容，这些内容保持与E-GOV CPS 和有关法律法规一致。

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吊销证书列表。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。

2.2 认证信息的发布

2.2.1 E-GOV CPS 的发布

HNCA E-GOV CPS 一经 HNCA 在网站（http://www.hnca.com.cn 和 http://www.9611111.com）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 1.5.4 的规定。有需要人士可访问 HNCA 网站（http://www.hnca.com.cn 和 http://www.9611111.com）查看，对具体个人不另行通知。

2.2.2 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服务器或指定的信息库位置中可查询获得证书和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。

HNCA的证书发布将利用LDAP目录服务器定时更新证书数据和CRL数据，并接收对证书及CRL的查询请求。

HNCA可根据电子政务信息系统的需要，依据双方的约定，将CA系统中签发、更新、重签发的数字证书定时或实时与电子政务信息系统进行数据同步，将证书信息同步到电子政务信息系统中。提供的信息可包括如下信息：业务类型、认证机构身份标识、订户基本信息、订户证书信息等。

HNCA可以根据需要，将CRL实时发布到指定的电子政务信息系统中。数据格式可包括如下信息：业务类型、认证机构身份标识、CRL文件、同步时间等。

2.3 发布时间或频率

2.3.1E-GOVCPS 的发布时间或频率

HNCA将及时发布E-GOVCPS的最新版本，一旦对规则的修改、补充、调整等获得批准，HNCA将在HNCA网站（http://www.hnca.com.cn和http://www.9611111.com）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-GOVCPS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-GOVCPS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。

2.3.2 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。

2.3.3 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。

通过发布服务器，请求者可以实时查看和获得某一证书的状态，包括有效状态、基于各种原因被注销、挂失的状态。

2.4 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。

3.身份标识与鉴别

3.1 命名

数字证书的命名遵循《电子政务数字证书格式规范》的要求。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。

3.1.1 DN 说明条款

1)DN必须能明确标识订户的真实身份；

2)单是主体名称不能唯一地标识客观实体；

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。

3.1.2 名称类型

每个订户对应一个甄别名。数字证书中主体的X.500 DN是C=CN命名空间下的X.500目录中唯一的名字。订户的甄别名(DN)必须具有一定的代表意义。

证书主体名称标识本证书所提到的最终实体的特定名称，描述了与主体公钥中的公钥绑定的实体信息。

3.1.3 订户的匿名或伪名

在HNCA证书服务体系中，订户证书申请人不允许使用匿名或伪名。

3.1.4 名称的唯一性

在HNCA证书服务体系中，证书主体名称必须是唯一的。

3.2 初始身份确认

3.2.1 证明持有私钥的方法

通过证书请求中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。在证书服务体系中，签名私钥在订户端生成，证书请求信息中包含用私钥进行的数字签名，用其对应的公钥来验证这个签名。

要求证书申请人妥善保管自己的私钥，因此，证书申请人视作其私钥的唯一持有者。

3.2.2 机构身份的鉴别

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。

机构身份的鉴别规范简要说明了如何进行组织身份鉴别。HNCA 保留根据最新国家政策法规的要求更新组织身份鉴别规范的权利。更新后的组织身份鉴别规

范将发布在HNCA的网站上(http://www.hnca.com.cn和http://www.9611111.com)。

对于机构身份的鉴别，需要查验机构的合法证照。

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、LRA提出申请。如该机构需申请含域名、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应妥善保存申请者的申请材料。

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。

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应妥善保存申请者的申请材料。

3.2.4 不予验证的订户信息

未在前面所列的，对于不影响订户身份追溯的信息，HNCA一般不予验证。

3.2.5 授权确认

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

3.2.6 审核认证体系成员身份确认

1）RA

RA所属企业必须为独立的法人机构，其身份审核依据本文3.2.2的要求进行，并由HNCA进行实地的考察后可确认其身份。

RA的资格由HNCA根据认证业务管理办法来审查批准，正式获得相应资格后，其运作遵循HNCA的相关规定。

2）业务受理人员

HNCA的业务受理人员必须是HNCA及所属RA机构的职员。

业务受理人员的身份除了必须符合个人证书申请者的条件外，还必须符合HNCA的相关规定。

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中心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HNCA E-GOV 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中心或电子认证服务机构的权力。

3.3 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)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。

2）等同采用§3.2身份的初始验证方法。

3.4 证书吊销请求的身份鉴别

数字证书订户申请吊销数字证书时，需要经过身份审核，才能够完成吊销过程。

HNCA可以采用以下方式来对吊销证书的订户身份进行鉴别：

1）用原证书提交合法有效的数字证书签名的吊销申请，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，无需再次进行其他形式的身份审核。

2）等同采用§3.2初始身份确认验证方法。

如果是因为订户没有履行 HNCA E-GOV CPS所规定的义务，由注册机构申请吊销订户的证书时，不需要对订户身份进行标识和鉴别。

4.证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

证书申请实体包括组织机构(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 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RA依据§3.2初始身份确认验证方法对证书申请人的身份进行鉴别，并决定是否受理申请。

申请过程中各方责任为：订户要按照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RA负责接收证书申请人的请求材料，当面对订户所提供的证书申请信息与身份证明资料的一致性进行查验。

HNCA数字证书申请流程为：

1）证书申请人从网上下载打印或从HNCA所属RA获取相应实体种类的数字证书申请登记表格，按表格要求填好申请表；或通过 HNCA 的在线服务系统提交申请信息。

2）依据§3.2初始身份确认验证方法鉴别申请人提交对应实体类型的证书申请登记表格及相关身份证明资料，到 HNCA 或其 RA 进行注册、身份审核和交费。

4.2 证书申请处理

4.2.1 身份审核

HNCA或其RA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审核。具体的鉴别流程详见§3.2。

4.2.2 证书申请批准和拒绝

HNCA或其RA对已通过身份审核的证书申请，并确认接收到相关费用款项，则批准证书申请，向HNCA提交证书签发请求。

证书申请人未能通过身份鉴证、未在约定时间内支付相关费用或为满足HNCA其他申请要求条件的，HNCA 或其 RA 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

一般情况下，HNCA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。或按双方约定的处理时限。HNCA允许未能提供足够身份证明材料的申请继续给予补充，这时将相应延长证书申请的处理时间。

HNCA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

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。HNCA 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。

HNCA 在确认为证书申请提交签发请求的 RA的身份后，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电子密钥中并进行证书发放，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。

4.3.2 电子认证服务机构对订户的通告

电子认证服务机构通过注册机构，对订户的通告有以下几种方式：

- 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。

4.4 证书接受

4.4.1 构成接受证书的方式

数字证书签发完成后，根据不同的业务操作流程，HNCA或其RA将数字证书本身、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，证书申请人即被视为同意接受证书。

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，就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已经签发的数字证书。

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。

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

4.5.2 依赖方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。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。

4.6 证书更新

证书中任何订户信息不变的情况下，为订户签发一张有效期更新后的数字证书。

4.6.1 证书更新的情形

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。

4.6.2 证书更新请求的处理

处理证书更新请求可以采用两种方式：

一种方式是在线自动更新。对于证书信息无须改变的订户，在证书即将过期时，在获得HNCA授权后，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。由注册机构来处理证书更新请求，为订户制作新的证书。

注册机构对申请证书更新订户的进行查验与鉴别，鉴别要求同本文§3.2.2和§3.2.3。

4.6.3 颁发新证书时对订户的通告

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§4.3.2规定相同。

4.6.4 构成接受更新证书的行为

证书更新后订户的证书接受与本文§4.4.1规定相同。

4.6.5 电子认证服务机构对更新证书的发布

证书更新的发布与本文§4.4.2规定相同。

4.7 证书密钥更新

证书密钥更新是指订户生成一对新密钥并申请为新公钥签发新证书，更新证书同时也会更新数字证书密钥。

4.7.1 证书密钥更新的情形

1)证书的有效期将要到期；

2)因私钥泄漏而吊销证书；

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。

4.7.2 证书密钥更新请求的处理

证书密钥更新请求的处理同§4.6.2。

4.7.3 颁发新证书对订户的通告

颁发新证书给订户的通告同§4.6.3。

4.7.4 构成接受密钥更新证书的行为

正式接受密钥更新证书的行为同§4.6.4。

4.7.5 电子认证服务机构对密钥更新证书的发布

HNCA 对密钥更新证书的发布同§4.6.5。

4.8 证书变更

证书变更是指证书订户的关键信息发生变化，导致证书内容有变化，需进行的重新登记和处理，但密钥对保持不变的情况。

4.8.1 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。

4.8.2 证书变更请求的处理

申请者到 HNCA 或其 RA 书面填写《HNCA 单位数字证书登记单》，并注明修改的原因；

HNCA 或授权的发证机构按照（§3.2）身份标识与鉴别办法对订户提交的证书修改申请进行审核；

证书签发后，发证机构将证书当面发给订户。订户接受证书(详看§4.4.1)；

新证书签发后原证书将被注销（§4.9）。HNCA 将在证书签发后 2 小时内在 LDAP 上发布订户的新证书。订户旧的证书在 24 小时内通过 CRL 发布。

4.8.3 颁发新证书时对订户的通告

颁发新证书对订户的通告同§4.6.3。

4.8.4 构成接受变更证书的行为

接受变更证书的行为同§4.4.1。

4.8.5 电子认证服务机构对变更证书的发布

变更证书的发布同§4.4.2。

4.9 证书吊销

4.9.1 证书吊销的情形

1）政务机构的证书订户工作性质发生变化；

2）政务机构的证书订户受到国家法律制裁；

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 的 RA 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雇员的私钥安全已经受到损害；

7）证书仅用于依赖主导的系统并由依赖方提出注销申请的；

8）证书密钥泄漏或存储证书的电子密钥丢失；

9）证书主体名称列明的从属关系改变；

10）证书主体的变更；

11）任何与提供证书服务相关的协议到期；

12）订户或其授权代表提出证书注销申请；

13）订户违反 HNCA E-GOV CPS 或签订的相关证书协议；

14）其它情况。例如因法律或政策等要求 HNCA 进行临时或永久性的证书注销措施。

证书的注销既可以是订户提出申请，也可以是 HNCA 因为订户的变更事实或违反约定事实而强行注销。

4.9.2 吊销请求的处理

证书吊销请求的处理采用与原始证书签发相同的过程。

1）证书吊销的申请人到HNCA或其授权的RA、LRA按要求填写《HNCA企业(个人)数字证书业务受理单》勾选“吊销”选项；

2）HNCA或其RA根据§3.2的要求对订户提交的吊销请求进行审核；

3）HNCA 吊销订户证书后，HNCA 或其 RA 将通知订户证书被吊销，订户证书在24小时内进入CRL，向外界公布；

4）强制吊销是指当 HNCA 或其 RA 确认订户有违反本E-GOV CPS的情况发生时，对订户证书进行强制吊销，吊销后将立即通知该订户。

4.9.3 吊销请求宽限期

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

4.9.4 证书挂起

HNCA暂不提供证书挂起服务。

4.9.5 证书吊销的发布

任何时候证书被吊销，HNCA在24小时内将该信息发布到HNCA信息库，并重新签发CRL。包含该吊销证书状态的CRL最迟在24小时内可以通过证书列明的URL获取。

当注销的证书过期时会被从下次发布的CRL中撤出。

4.9.6 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，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。

2）OCSP查询：服务系统接受证书状态查询请求，从目录服务器中查询证书的状态，查询结果经过签名后，返回给请求者。

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。

4.10 证书状态服务

4.10.1 操作特点

订户和依赖方可以从HNCA网站或者目录服务器下载CRL查询证书状态，或者使用HNCA或者第三方的OCSP客户端工具进行在线证书状态查询。

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。

4.10.3 可选特征

根据请求者的要求，在请求者支付相关费用后，HNCA可以提供以下通知服务：

1)收到证书主题的电子签名消息的接受者要求，确认该证书是否已被吊销；

2)提供通知服务，当指定的证书被吊销时，HNCA将通知请求该项服务的请求者。

4.11 订购结束

订购结束是指当证书有效期满或证书吊销后，该证书的服务时间结束。

订购结束包含以下两种情况：

1)证书有效期满后，订户不再延长证书使用期或者不再重新申请证书。与未到期的其他注销订户对比，其证书不会进入CRL；

2)在证书有效期内证书被吊销，并不再更换新的证书。

4.12 密钥生成、备份与恢复

4.12.1 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生成或由HNCA提供的密码设备（如智能USB KEY或智能IC卡）生成，HNCA 任何所属机构不对该密钥对进行备份；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）产生，并在KMC备份托管。

4.12.2 密钥的恢复

密钥恢复是指加密密钥的恢复，密钥管理中心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。订户在HNCA授权的发证机构申请，经§3.2身份验证所述身份证明材料鉴别验证审核后，通过HNCA向KMC请求；密钥恢复模块接受订户的恢复请求，恢复订户的密钥并下载于订户证书载体中。

2）司法取证密钥恢复：司法取证人员在KMC申请，经§3.2身份验证所述身份证明材料鉴别验证审核后，由密钥恢复模块恢复所需的密钥并记录于特定载体中。

4.12.3 密钥对的存储和恢复安全策略

私钥在KMC生成后始终以加密的状态存储在密钥库中，且每个私钥由硬件加密设备生成不同的会话密钥进行加密。

对于每次密钥对的申请和恢复，KMC使用订户或HNCA提供的电子密匙产生的公钥对所申请（或恢复）的私钥进行加密传送，保持中间任何环节私钥都不会被获取。

具体策略在§6.1和§6.2中详细描述。

4.12.4 会话密钥的封装与恢复的策略和行为

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

5.认证机构设施管理和操作控制

5.1 物理控制

5.1.1 机房的建筑

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。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。

5.1.2 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。并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,指纹、密码双因素控制、可控权限和时间的门禁系统等监控技术；以及人工监控管理，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 设置指纹和密码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。

对于非业务管理和系统维护人员，只有经 HNCA 安全管理小组授权的工作人员陪同下,并获得 HNCA 安全管理小组负责人批准,才可进入相应限制区域活动，并且一切活动皆由摄像监控设备及系统监控软件记录。

5.1.3 电源和空调

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。

5.1.4 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。

5.1.5 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。

5.1.6 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。

5.1.7 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，进行销毁。

5.1.8 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。

5.1.9 入侵红外报警系统

HNCA 在 CA 机房内部署了入侵红外报警系统，并进行安全布防。

5.2 操作过程控制

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：

1)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，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。

2)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。

3)审计管理员

审计管理员控制、管理、使用安全审计系统，安全审计系统分布于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。

4)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。

5)证书业务管理员

证书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。

6)证书业务操作员

证书业务操作员进行录入、审核、制作等证书业务操作，直接对用户提供服务。

7)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，直接对用户服务。

5.2.2 角色要求的人数

HNCA 对于涉及敏感信息的操作任务，要求采取双人控制策略，并为担任该任务角色至少配置 3 人。某些涉及敏感信息的区域的进入也是采取双人控制策略（见本文 5.1.2）；核心秘密（如 CA 根密钥）分管者和操作的物理访问控制者由不同的人员担任角色。

5.2.3 可信角色的鉴别

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，或在有进入该区域权限的可信人员的陪同下进入，并持有经授权的智能 IC 卡和证书进入系统进行相应业务的操作和管理。

5.2.4 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)从事证书申请信息验证的人员；

2)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；

3)负责证书签发、撤销等工作或者能够访问受限、敏感信息的人员；

4)负责处理订户信息的人员；

5)负责生成、签发和销毁CA系统证书的人员；

6)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、制证员3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 人员资格要求

所有的员工与 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。

5.3.2 背景调查程序

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犯罪记录、社会关系和社会安全方面的调查。

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)考核合格报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、HNCAE-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。

5.3.4 再培训要求

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 对未授权操作的处理

HNCA 员工所有涉及到业务操作安全的操作均有记录。记录由 HNCA 系统管理员或安全管理员审查。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。

5.4 审计日志程序

5.4.1 记录事件的类型

HNCA 日志记录的事件包括但不限于以下内容：

- 涉及 CA 密钥发生的事件。包括密钥生成、备份、存储、恢复、归档、销毁，密码设备的启用、停用、转移和销毁。

- 涉及数字证书发生的事件。包括证书的申请、更新、密钥更新、密钥恢复、挂失/取消挂失、注销，证书业务申请的审核通过或拒绝，证书的签发、接受、CRL 的签发。
- 涉及网络安全的事件，包括防火墙、路由器、入侵检测记录的信息，以及被攻击的相应处理记录。
- 其它安全事件。包括各系统的登录、退出，系统的各种配置及其修改，业务处理的成功或失败，系统部件的安装、升级、维修，人员在各区域的访问记录，敏感信息的取阅。

每个事件的记录至少包括以下信息：

- 发生的日期和事件。
- 事件的内容。
- 事件相关的实体。
- 事件的标识。

5.4.2 日志的处理周期

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

只有被 HNCA 授权的人员才能对日志进行查看和处理，HNCA 对系统的日志设有访问控制权限。

5.4.5 审计日志的备份

HNCA 定期对纸质日志实施归档，对电子日志实施备份(周期参见本文 5.4.3)。归档或备份的日志都会被保存在同城异地，并需要授权才能取阅或恢复。

5.4.6 审计日志的采集

HNCA 的审计日志分手工采集和自动采集两种方式。自动采集的主要是电子日志，通过 CA 系统（包括各子系统）、网络设备、各计算平台产生并记录；手工采集的主要是纸质日志，通过操作或出入人员的手工记录产生。

5.4.7 对导致事件实体的通告

HNCA 将依据法律、法规的监管要求，可能对一些恶意行为，如网络和病毒攻击等，通知相关的主管部门，并且 HNCA 保留进一步追究责任的权利。

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 归档记录种类

HNCA 归档的记录包括本文 5.4 所述的所有日志记录和证书数据库文件、CA 密钥备份、HNCA 发行的证书、CRL、ARL、证书各种业务申请资料等。

5.5.2 档案保存期限

HNCA 的档案保存期限至少为档案相关证书或密钥失效后 10 年。

5.5.3 档案的保护

HNCA 的档案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。

5.5.4 档案备份

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 档案的标识

对于每一个 HNCA 的档案，都给予适当标识，标识的内容包括：编号、归档时间、档案内容、经办人等。

5.5.6 档案采集系统

HNCA 的档案采集系统分为人工处理和自动处理两部分组成。

5.5.7 档案验证

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。

5.6 CA 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。

5.7 损害和灾难恢复

5.7.1 HNCA 遭攻击或发生损害事故时的恢复程序

HNCA 备份所有 CA 运行所需的数据、软件和资料。当发生事故或受到攻击时，用于系统的复原。HNCA 制定相关的安全事件诊断和处理程序，包括业务连续性计划、灾难恢复程序等。

5.7.2 计算资源、软件或数据的破坏处理

当出现计算资源或软件或数据被破坏，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，作恢复处理。必要时可能启动 CA 私钥损害处理或灾难恢复程序。

5.7.3 CA 私钥损害的处理

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。

5.7.4 灾难发生后的业务保持

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 CA 或 RA 业务终止

5.8.1 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。

5.8.2 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。

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

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 KMC 的密码设备产生。

6.1.2 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，保证传递中间环节加密私钥不泄露。

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。

6.1.3 公钥的传递

订户的公钥采用证书签发请求格式（PKCS#10）或其它专门的安全格式通过安全通道传递给 HNCA 完成证书签发。订户证书签发后其公钥再随证书由 HNCA 发布到 HNCA 的证书库，证书依赖方可以从 HNCA 证书库下载该公钥。

HNCA 的公钥或其直接生成证书的公钥，则直接由 HNCA 签发证书后随证书发布到 HNCA 证书库供订户和依赖方下载。

6.1.4 密钥长度

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根据用户需求为订户签发不同算法类型和密钥长度的证书。

6.1.5 公钥参数的产生

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。

6.1.6 密钥用途

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

HNCA 的签名密钥用于签发下级 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。

6.2 私钥保护与密码模块的控制

6.2.1 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。

6.2.2 私钥的分割管理

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。

6.2.3 私钥托管

HNCA 的根和下级 CA 的私钥不进行托管，其它的签名私钥也都不进行托管。根据国家相关法规的要求，HNCA 代订户向 KMC 申请加密密钥对的托管，其服务和安全保证参见本文 4.12 节。订户的签名私钥自行管理，以保证其不可否认性。

6.2.4 私钥备份

HNCA 的私钥按本文 6.2.2 的管理方式备份到安全介质中（如 IC 卡），以作灾难恢复或密码设备更换时的恢复。 除第 6.2.3 的托管服务外，HNCA 不对订户的私钥进行备份。

6.2.5 私钥归档

HNCA 对过期的 CA 密钥对进行归档，保存期限按照本文 5.5.2 的要求。已归档的 CA 私钥不再利用，并在保存期过后进行销毁。依据国家相关法规或 HNCA 与订户的协议，KMC 可对不再托管的私钥进行归档。

6.2.6 私钥在密码模块中的导入和导出

HNCA 的 CA 私钥可以在密码模块中导出，以实现私钥备份；HNCA 的 CA，也可以导入到其它由国家密码主管部门许可的密码模块中，以实现灾难恢复和密码设备更新等。

订户可以使用 HNCA 提供的硬件密码设备，使其私钥无法从电子密匙中导出，确保订户私钥的安全；但订户的加密私钥可以导入到电子密匙中。

6.2.7 私钥在密码模块中的保存

私钥在硬件密码设备中是以密文的形式保存。

6.2.8 私钥的激活

HNCA 的私钥采用本文 6.2.2 的控制方式进行激活，并每次请求私钥运算时需提供口令。

订户的私钥保存在电子密钥或智能卡中，需要提供 PIN 码才能激活私钥。部分硬件密码设备的私钥激活可配置成一定周期后自动失效（停止）。

6.2.9 私钥的停止

所有硬件密码模块断电后或从接口中拔出后，私钥的激活状态将自动停止（取消激活）。HNCA 的私钥还可采用本文 6.2.2 的控制方式进行停止。停止状态下私钥仅以密文的形式存在。

6.2.10 私钥的销毁

HNCA 对归档期过后的私钥进行销毁，包括保存在硬件密码设备中的副本及其使用备份，HNCA 确保这种销毁是不可复原的。HNCA 采用本文 6.2.2 的控制方式销毁硬件密码设备中的私钥。

HNCA 对从订户中回收的硬件密码设备进行私钥销毁。订户在停止使用证书加解密功能的情况下，为防止密钥泄漏及可能发生的密钥盗用情况，也可以使用 HNCA 提供的证书管理工具的删除功能销毁私钥。

6.3 密钥对的其它管理

6.3.1 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第三方的数据库中，并在其失效后仍会在 HNCA 系统中保存至少 10 年。

6.3.2 密钥对与证书的有效期

一般情况下密钥对的有效期视为与其对应的证书有效期相同。密钥对到期后不能再作为签名和加密使用，但可以继续用来验证签名和解密信息。

6.4 激活数据

6.4.1 激活数据的产生

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 6.2.2）。初始的口令或 PIN 码通常由 HNCA 产生，或是预制的，或是由计算机随机产生的。HNCA 要求其业务人员或建议订户按以下规则设置或修改口令和 PIN 码：

长度不小于 8 个字符，除非系统或设备限制；

由数字、字母和特别符号（如“*&%$#@\~!”）组成；

不使用有含义的字串；

不能和操作员的名字相同；

不能包含订户名信息中的较长的子字符串；

不使用用过的口令或 PIN 码。

6.4.2 激活数据的保护

对于“秘密分享”，其持有者将遵守规定存放在具有物理保护的地方。口令和 PIN 码只有授权的私钥使用人员才能知悉。需要传递的口令和 PIN 一般使用密码信封，防止泄露或被窃取。 激活数据被猜测或攻击时（如多次输入不正确的口令或 PIN 码），将被自动锁死。 HNCA 在任何时候发现其激活数据可能泄露的

情况下，对激活数据进行更改，并销毁存在的记录，不对历史激活数据归档。订户应自行评估其电子密匙的 PIN 码的泄露情况，建议订户定期更换 PIN 码。

6.5 计算机安全控制

6.5.1 计算机安全性要求

HNCA 用于运行认证系统和处理数据的生产用计算机由 HNCA 的系统管理员维护，只有系统管理员或专门授权人员才能管理这些计算机（包括软件安装、卸载、系统优化、部件更换等），以保证系统处于安全可信的运行状态。

HNCA 生产用计算机安装有病毒保护程序，并定时更新防病毒软件的病毒库。任何维护时需接入生产网络的计算机均需进行病毒清查后才能使用。 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有最小密码长度要求，而且必须符合复杂度要求，系统管理员定期更改这些口令。

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

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。

6.6.2 系统改进控制

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，并只有授权的工程实施人员才能访问；认证系统的升级需由安全管理小组批准。HNCA 在实施补丁或升级之前对代码进行验证，包括测试和版本核对。

6.6.3 安全管理控制

HNCA 认证系统的配置以及任何修改都会记录在案，并制定相关的管理程序和监督机制，包括确定认证系统的访问角色、制定网络安全策略、制定认证系统的访问机制、制定认证系统的审计机制等，来保障认证系统配置的安全，防止未授权的修改。

6.7 网络安全性控制

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。

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、CRL 和发布服务

7.1 证书

HNCA签发的证书格式，符合GM/T 0015-2012或ITU-T X.509 V3。

7.1.1版本号

证书版本号为 X.509 V3。

7.1.2 证书扩展项

HNCA 也支持 GB/T 20518 标准及电子政务数字证书格式标准中指定的标准扩展，并支持订户自定义私有扩展，可根据订户或应用的要求定制。私有扩展一般情况下为非关键项。

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

7.1.3 算法 OID

1)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：OID1.2.156.10197.1.501

2)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：OID1.2.156.197.1.411

SM3 的对象标识符位：OID1.2.156.197.1.401

3)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

4)对称算法

SM1 对象标识符为：OID 1.2.156.197.1.102

SM4 对象标识符为：OID1.2.156.197.1.104

SSF33 对象标识符：OID1.2.156.197.1.103

7.1.4 名称形式

HNCA 数字证书中的主体 Subject 的 X.500 DN 是 C=CN 命名空间下的 X.500 目录唯一名字，各属性的编码一律使用 UTF8String。

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

C=CN;

OU=××;

O=××;

L=××;

S=××;

CN=××;

CN（common name）证书使用者名称

OU(Organization Unit)应为证书主体或者证书主体所属单位的名称全称；（非必选）

O(Organization)证书主体或者证书主体所属单位具有明确的上一级单位，则应为其上一级单位的名称全称；（非必选）

L（Location）为证书主体所属单位的省辖市；

S 所在省、自治区、直辖市名称全称；

C（Country）应为 CN，表示中国；

CN（Common Name）中的内容分为 4 种：

1)个人证书中应为证书主体的姓名；

2)单位机构证书中应为证书主体单位的名称或企业税务登记号；

3)服务器证书应为证书主体设备的域名或者 IP 地址；

4)代码签名证书应为负责人的姓名，或者是所属单位的名称。

7.1.5 证书密钥用法

HNCA 根据国家密码管理局的相关要求,严格规定数字证书的密钥用法。HNCA 签发的数字证书中都在密钥用法（Key Usage）中明确指明了此已认证的公开密

钥可用于何种用途。订户和依赖方必须根据证书的密钥用法严格控制数字证书的使用场景。

7.2 CRL

HNCA 发布的 CRL 符合《GB/T 20518-2006 信息安全技术 公钥基础设施 数字证书格式》及 ITU-T X.509、RFC 5280 标准规范。

7.2.1 版本号

CRL 版本号为 X.509 V2。

7.2.2CRL 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 发布服务

HNCA 采用 OCSP 提供证书状态查询服务。发布服务作为 CRL 的有效补充，提供比 CRL 较为及时的证书状态查询机制，方便订户及时的获取证书状态信息。HNCA 的发布服务系统符合 RFC2560 标准规范。

7.3.1 版本号

发布服务系统版本号为 V 1。

7.3.2 OCSP 扩展项

HNCA 未使用 OCSP 相关扩展项。

8.认证机构审计和其他评估

HNCA 建立内部审计机制，并组织信息安全风险评估活动。HNCA 还接受国家电子认证服务主管部门组织的年度审查。其它第三方的外部审计或评估依据客户协议或其它政策进行。

8.1 审计的依据

审计是为了检查和监督 HNCA 及其下属机构或其它关联机构是否依据《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子政务电子认证服务业务规则》的要求，依法开展电子认证服务业务，以及在开展业务过程中，是否存在违反其它法律法规以及 HNCA 的业务规范、管理制度、安全策略等情况，以达到规避经营风险、提高服务质量、保障客户权益的目的。

8.2 审计的形式

审计分为外部审计与内部审计。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 HNCA 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。内部审计是指 HNCA 自行组织人员对机构内部、下属机构等进行审计评估，审计结果供内部用以完善管理、改进服务，不需对外公开。

8.3 审计或评估的频率

HNCA 的内部审计周期为每年一次，并且每年进行两次信息安全的脆弱风险评估。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。

8.4 审计或评估人员的资质

HNCA 的内部审计或评估人员要求熟悉电子认证业务和 PKI 技术体系，接受过内部信息安全管理培训，并由安全管理小组任命。外部审计或评估人员的资质由相关法规或主管部门确定。

8.5 审计或评估人员与 HNCA 的关系

HNCA 内部审计人员要求与被审计对象无责任关系，为 HNCA 雇员。HNCA 内部风险评估的负责人要求与被评估对象无责任关系，可以是 HNCA 雇员，也可以是非 HNCA 雇员。外部审计或评估人员应为与 HNCA 无任何除审计或评估之外的业务、财务往来或其他足以影响评估客观性的利害关系。

8.6 审计或评估的内容

HNCA 内部审计或评估涉及的内容包括以下：

- 人员管理
- 物理环境建设及安全管理
- 系统结构及其运行管理
- 密钥管理
- 客户服务规范管理

综合运营规范（如法规、E-GOV CPS、风险控制等方面）在特殊情况下的审计或评估内容可能只包括以上内容的一部分。国家电子认证服务主管部门组织的年度审查内容遵照其发布的最新要求。

8.7 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有不足或存在问题，HNCA 将根据审计或评估报告制定和实施纠正措施，并由安全管理小组监督执行。对于重大的安全隐患，HNCA 同样会启动应急事件处理程序，以迅速控制风险的影响范围。

8.8 审计或评估结果的传达与发布

HNCA 只按管理或协议要求将审计或评估结果传达到相应对象。 除非法律法规要求，HNCA 一般不公开审计或评估结果。

9.法律责任和其它业务条款

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价格政策，并在网站http://www.hnca.com.cn和http://www.9611111.com上予以公布。如价格政策有任何变化，HNCA将及时更新发布。

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。

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，并在用户订购时提前告知。

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 证书吊销或状态信息查询费用

HNCA对证书撤销和状态查询，目前不收取任何费用。

9.1.4 其它服务费用

HNCA保留收取其他服务费的权利。

9.1.5 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。

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 保密信息的范围

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。

9.3.2 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 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。

9.3.3 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 授权的人员才能接近机密信息。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 9.3.1 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。

9.4 个人隐私保密

9.4.1 隐私保护方案

HNCA 制定隐私保护策略，所有相关人员（包括 HNCA 及其 RA 的工作人员、订户等）必须严格遵守相应的规章制度。HNCA 根据国家相关法规的出台，及时调整隐私保护策略，以符合国家法规的要求。

9.4.2 作为隐私处理的信息

由 HNCA 接收到的不在证书、CRL 体现的证书申请者（包括联系人）、订户的相关信息均作为隐私信息处理。

9.4.3 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。

9.4.4 保护隐私信息的责任

HNCA 对本文 9.4.2 所列的隐私信息进行保护，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。

9.4.5 使用隐私信息的告知与同意

HNCA 只在其业务范围内使用本文 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。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，并负担相应的行政、经济责任。

9.4.6 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本文 9.4.2 中的隐私信息时，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。

9.4.7 其他信息披露情形

当隐私信息其本人出于某种原因，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。

9.5 知识产权

9.5.1 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。

9.5.2 HNCA 使用其他方知识产权的声明

HNCA 在其服务系统中使用的软硬件设备、辅助设施和相关操作手册，其知识产权为相关供应商所有，HNCA 保证都是合法的拥有相应权利。

订户或证书申请人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。

9.6 陈述与担保

9.6.1 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领导，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。
- 除了未经验证的订户信息外,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，及时注销证书，并签发 CRL。
- 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。

9.6.2 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。
- 除了未经验证的订户信息外,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。

9.6.3 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或其它合法的使用目的。
- 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。

9.6.4 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。

9.7 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 9.16.5 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。

9.8 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。

9.9 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 产生损失，则订户或依赖方应承担赔偿责任。

9.9.1 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。

9.9.2 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冒然信任证书及其行为，而造成 HNCA 或其他方遭受损害的。

9.10 有效期限与终止

9.10.1 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。

9.10.2 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。

9.10.3 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。

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E-GOV CCPS不适用时，由HNCA策略管理委员会委托执行小组对CPS进行修订。策略管理委员会执行小组负责起草新的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策略管理委员会审阅；执行小组依据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。

9.12.2 通告机制和期限

本E-GOVCPS在HNCA网站http://www.hnca.com.cn和http://www.9611111.com上发布。

版本更新时，最新版本的E-GOV 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 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。

9.13 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。

9.14 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。

9.15 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》、《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。

9.16 一般条款

9.16.1 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。

9.16.2 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 之所属订户须按国家规定，接受相应接管 CA 的证书服务条款。

9.16.3 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。

9.16.4 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。

9.16.5 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；再如战争、罢工、骚乱等社会异常事件。

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。

9.17 其它条款

9.17.1 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的范围内；
- 该冲突的协议的签署日期在 HNCA E-GOV CPS 首次公开发行之前；
- 该冲突的协议明确地优于 HNCA E-GOV CPS。

9.17.2 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。

9.17.3 损害性资料

证书申请人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。

10.支持服务管理

10.1 服务内容

HNCA将提供面向证书订户和面向应用提供方的服务支持。

10.1.1 面向证书持有者订户的服务支持

1）数字证书管理：包括数字证书的导入、导出、客户端证书管理工具的安装、使用、卸载等。

2）数字证书应用：基于数字证书的身份认证、电子签名、加解密等应用出现的证书无法读取、签名失败、证书验证失败等应用问题。

3）证书存储介质硬件设备使用：包括证书存储介质使用过程中出现的口令锁死、驱动安装、介质异常等。

4）电子政务电子认证服务支撑平台使用：为订户提供数字证书在线服务平台使用中的各类问题，包括：证书更新失败、下载异常、无法提交注销申请等。

10.1.2 面向应用提供方的服务支持

1）电子认证软件系统使用：提供受理点系统、注册中心系统、LDAP、OCSP、信息服务系统等系统的使用支持，如证书信息无法查询、数据同步失败、服务无响应等。

2）电子签名服务中间件的应用：解决服务中间件的集成时出现的诸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。

10.2 服务方式

10.2.1 坐席服务

HNCA设置有服务热线。热线坐席根据订户的问题请求，协助订户处理。

10.2.2 在线服务

HNCA通过以下方式为电子政务证书订户和应用提供方提供在线服务：

- 自助信息查询
- 网络实时通讯
- 远程终端协助
- 在线方式和传统模式的结合

10.2.3 现场服务

根据服务协议的约定，由HNCA技术工程师和客户服务人员上门为订户处理数字证书应用中存在的问题。

10.2.4 满意度调查

通过电话、WEB网站、邮件系统、传真等多种订户可接受的方式不定期地开展订户满意调查，分析调查结果，改善服务。

10.2.5 投诉处理

向订户公布投诉电话和传真，并通过WEB网站等方式，收集和受理订户投诉，并对投诉处理过程进行记录。投诉处理的结果将及时反馈给订户。

10.2.6 培训

HNCA可依据与客户的约定进行培训。培训内容可以包括以下内容：电子政务电子认证服务基础性技术知识、客户服务规范、数字证书应用集成规范、常见问题解答（FAQ）、操作使用手册等。

10.3 服务质量

HNCA的坐席服务、在线服务、现场服务时间做到充分满足订户的需要。服务时间满足7*12小时。视双方服务协议的约定，可提供延长服务时间。

HNCA对于技术问题和客服问题均按照问题类别、严重程度依次分类登记和处理，制定响应处理流程和工作机制，确保服务的及时性和连续性，各类响应时间可按双方约定，以不影响客户使用数字证书为准则。

10.4 证书应用集成支持服务

10.4.1 证书应用集成内容

HNCA 具备针对电子政务信息系统的电子认证安全需求分析的能力，电子认证法律法规、技术体系的咨询能力以及设计满足业务要求的电子认证及电子签名服务方案设计能力。HNCA 数字证书应用方案设计包括：证书格式设计、证书交付、支持服务、信息服务、集成方案、建设方案、介质选型等。

HNCA 证书应用集成主要包括：

- 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；
- 制定项目管理制度，规范系统和程序开发行为；
- 制定安全控制流程，明确人员职责；
- 实施证书软件发布版本管理，并进行证书应用环境控制；
- 项目开发程序和文档等资料的妥善归档保存。

10.4.2 证书应用接口

HNCA 证书应用接口为上层应用提供简捷、易用的调用接口，该接口符合《电子政务数字证书应用接口规范》，提供证书环境设置、证书解析、随机数生成、签名验证、加解密、数据服务接口等功能。

其主要包括服务器端组件接口和客户端控件接口。服务器端组件和客户端控件支持不同认证机构所签发的符合《电子政务数字证书格式规范》的数字证书。

HNCA 证书应用接口程序支持 Windows、AIX、Solaris、Linux 等多种系统平台，并提供 C、C＃、Java 等多种接口形态，可通过 com 组件、java 组件、ActiveX 控件、Applet 插件等多种形态提供服务。

10.4.3 证书应用集成服务

HNCA 为电子政务应用单位提供证书应用接口程序集成工作。集成工作主要包括以下服务：

- 提供证书应用接口的开发包（包括客户端和服务器端）；
- 接口说明文档；
- 集成演示 Demo；
- 集成手册；
- 证书应用接口开发培训和集成技术支持；
- 协助应用系统开发商完成联调测试工作。

10.4.4 决策支持信息服务

根据服务协议的约定，HNCA 可通过 Web 或 WebService 方式面向应用系统提供方提供以下决策支持信息服务：

- 订户档案信息：分业务、地域、时段等提供订户信息的统计分析服务；
- 投诉处理信息：提供特定业务、时间、特定订户群、问题类别等的汇总信息及分析；
- 客户满意度信息：提供面向业务的客户满意度调查信息；
- 服务效率信息：提供面向业务的服务效率分析信息，如处理时间、服务接通率等。