

河南信安 CA
电子认证业务规则
(正式版本3.4)

(生效日期：2023年1月11日)

河南省信息化集团有限公司
Henan Province Information Group Co., Ltd

河南信安CA电子认证服务业务规则版本说明

河南省信息化集团有限公司电子认证服务业务规则如表1所示：

版本	发布日期	备注
3.4	2022年01月11日	依据业务发展情况，进行修订。
3.3	2022年09月27日	依据业务发展情况，进行修订。
3.2	2021年08月03日	依据业务发展情况，进行修订。
3.1	2021年03月19日	依据业务发展情况，进行修订。
3.0	2019年07月17日	依据业务发展情况，进行修订。
2.0	2017年01月05日	依据业务发展情况，进行修订。
1.0	2013年01月21日	依据《电子认证服务业务规则规范》制定

注：河南省信息化集团有限公司已发布最新版本为V3.4。

表1：河南省信息化集团有限公司电子认证服务业务规则版本。

目 录

1 概括性描述	1
1.1 概述	1
1.2 文档名称与标识	1
1.2.1 名称.....	1
1.2.2 版本.....	1
1.3 认证体系的成员	1
1.3.1 电子认证服务机构.....	2
1.3.2 注册机构.....	2
1.3.3 订户.....	3
1.3.4 依赖方.....	3
1.3.5 其他成员.....	3
1.4 证书应用	3
1.4.1 证书性质.....	4
1.4.2 禁止的证书应用.....	4
1.5 策略管理	4
1.5.1 策略文档管理机构.....	4
1.5.2 联系信息.....	4
1.5.3 决定CPS符合策略的机构.....	4
1.5.4 CPS批准流程.....	4
1.6 定义和缩写	5
2 信息发布与信息管理	10
2.1 信息库	10
2.2 认证信息的发布	10
2.2.1 CPS的发布.....	10
2.2.2 证书和CRL发布.....	10
2.3 发布时间或频率	11
2.3.1 CPS的发布时间或频率.....	11
2.3.2 证书的发布时间或频率.....	11
2.4 对信息的访问控制	11
3 身份标识与鉴别	13
3.1 命名	13
3.1.1 名称类型.....	13
3.1.2 对名称的意义化要求.....	13
3.1.3 订户的匿名或伪名.....	13
3.1.4 理解不同名称形式的规则。.....	13
3.1.5 名称的唯一性.....	13
3.1.6 商标的承认、鉴别和角色.....	14

3.1.7 各类数字证书 CN 的取值方式	14
3.2 初始身份确认	14
3.2.1 证明拥有私钥的方法	14
3.2.2 机构的身份确认	14
3.2.3 个人的身份确认	16
3.2.4 不予验证的用户信息	17
3.2.5 审核认证体系成员身份确认	17
3.2.6 互操作原则	17
3.3 证书（密钥）更新请求中的身份鉴别	18
3.3.1 常规密钥更新的标识与鉴别	18
3.3.2 吊销后密钥更新的识别预报鉴别	18
3.4 证书吊销请求中的身份鉴别	18
4 证书生命周期操作规范	19
4.1 证书申请	19
4.2 证书申请处理	19
4.2.1 身份审核	19
4.2.2 证书申请的接受与拒绝	19
4.2.3 处理证书申请的时间	19
4.3 证书签发	20
4.4 证书接受	20
4.4.1 证书的发布	20
4.4.2 接受证书的方式	20
4.5 密钥对和证书的使用	21
4.5.1 用户私钥和证书的使用	21
4.5.2 依赖方对他人证书和公钥的使用	21
4.6 证书更新	21
4.6.1 证书更新的情形	21
4.6.2 证书更新请求的处理	22
4.6.3 证书更新的签发、发布和用户接受	22
4.7 证书密钥更新	22
4.7.1 证书密钥更新的情形	22
4.7.2 证书密钥更新请求的审核	22
4.7.3 证书密钥更新的签发、发布和用户接受	23
4.8 证书变更	23
4.8.1 证书变更的内容	23
4.8.2 证书变更请求的审核	23
4.8.3 证书变更的签发、发布和用户接受	23
4.9 证书的吊销和挂起	23
4.9.1 证书吊销的情形	23
4.9.2 请求证书吊销的实体	24
4.9.3 吊销请求的流程	24
4.9.4 吊销请求的宽限期	24

4.9.5 证书挂起的处理	25
4.9.6 证书吊销和挂起状态的发布	25
4.9.7 依赖方检查证书状态的要求	25
4.10 证书状态服务	25
4.11 订购结束	25
4.12 密钥生成、备份和恢复	26
4.12.1 密钥的生成和备份	26
4.12.2 密钥的恢复	26
4.12.3 密钥对的存储和恢复安全策略	26
5 认证机构设施、管理和操作控制	27
5.1 物理控制	27
5.1.1 机房的建筑	27
5.1.2 物理访问	27
5.1.3 电源和空调	27
5.1.4 水患防治	28
5.1.5 火灾预防和保护	28
5.1.6 介质存储	28
5.1.7 废物处理	28
5.1.8 异地备份	28
5.1.9 入侵侦测报警系统	29
5.2 操作过程控制	29
5.2.1 可信角色	29
5.2.2 角色要求的人数	29
5.2.3 可信角色的鉴别	29
5.2.4 职责需分离的角色	30
5.3 人员控制	30
5.3.1 人员资格要求	30
5.3.2 背景调查程序	30
5.3.3 培训要求	30
5.3.4 再培训要求	31
5.3.5 工作轮换周期和顺序	31
5.3.6 对未授权操作的处理	31
5.3.7 独立合约人要求	31
5.3.8 提供给员工的文档	31
5.4 审计日志程序	32
5.4.1 记录事件的类型	32
5.4.2 日志的处理周期	32
5.4.3 审计日志的保存期限	32
5.4.4 审计日志的保护	32
5.4.5 审计日志的备份	33
5.4.6 审计日志的采集	33
5.4.7 对导致事件实体的通告	33
5.4.8 脆弱性评估	33
5.5 记录归档	33
5.5.1 归档记录种类	33

5.5.3 档案的保护	33
5.5.4 档案备份	33
5.5.5 记录时间戳的要求	34
5.5.6 档案采集系统	34
5.5.7 获得和检验归档信息程序	34
5.6 电子认证服务机构密钥更替	34
5.7 损害和灾难恢复	34
5.7.1 HNXACA 遭攻击或发生损害事故时的恢复程序	34
5.7.2 计算资源、软件或数据的破坏处理	34
5.7.3 CA 私钥损害的处理	35
5.7.4 灾难发生后的业务保持	35
5.8 CA 或 RA 业务终止	35
5.8.1 CA 业务终止	35
5.8.2 注册机构业务终止	36
6 认证系统技术安全控制	37
6.1 密钥对的生成和安装	37
6.1.1 密钥对的生成	37
6.1.2 私钥的传递	37
6.1.3 公钥的传递	37
6.1.4 电子认证服务机构公钥传输给依赖方	37
6.1.5 密钥长度	37
6.1.6 公钥参数的产生	38
6.1.7 密钥用途	38
6.2 私钥保护与密码模块的控制	38
6.2.1 密码模块标准与控制	38
6.2.2 私钥的分割管理	38
6.2.3 私钥托管	39
6.2.4 私钥备份	39
6.2.5 私钥归档	39
6.2.6 私钥在密码模块中的导入和导出	39
6.2.7 私钥在密码模块中的保存	39
6.2.8 私钥的激活	39
6.2.9 解除私钥激活状态的方法	40
6.2.10 私钥的撤销	40
6.2.11 密码模块的评估	40
6.3 密钥对的其他管理	40
6.3.1 公钥归档	40
6.3.2 密钥对与证书的有效期	40
6.4 激活数据	40
6.4.1 激活数据的产生	40
6.4.2 激活数据的保护	41
6.5 计算机安全控制	41
6.5.1 计算机安全性要求	41
6.5.2 计算机的安全等级	42

6.6 生命周期技术控制	42
6.6.1 系统开发控制	42
6.6.2 系统改进控制	42
6.6.3 生命周期的安全控制。	42
6.7 网络安全性控制	42
7 证书、CRL 和 OCSP	44
7.1 证书	44
7.1.1 版本号	44
7.1.2 证书扩展项	44
7.1.3 算法 OID	44
7.1.4 名称形式	44
7.1.5 证书密钥用法	45
7.1.6 证书策略 OID	45
7.1.7 策略限定符的语法和语义	45
7.2 CRL	45
7.2.1 版本号	45
7.2.2 CRL 和 CRL 条目扩展项	45
7.3 OCSP	46
7.3.1 版本号	46
7.3.2 OCSP 扩展项	46
8 认证机构审计和其他评估	47
8.1 审计的依据	47
8.2 审计的形式	47
8.3 审计或评估的频率	47
8.4 审计或评估人员的资质	47
8.5 审计或评估人员与 HNXACA 的关系	48
8.6 审计或评估的内容	48
8.7 对问题与不足采取的措施	48
8.8 审计或评估结果的传达与发布	48
9 法律责任和其他业务条款	49
9.1 费用	49
9.1.1 证书签发和更新费用	49
9.1.3 证书状态信息查询费用	49
9.1.4 其他服务费用	49
9.1.5 退款政策	49
9.2 财务责任	49

9.3 业务信息保密	50
9.3.1 保密信息的范围	50
9.3.2 不在保密范畴内的信息	50
9.3.3 保护保密信息的信息	50
9.4 个人隐私保密	51
9.4.1 隐私保护方案	51
9.4.2 作为隐私处理的信息	51
9.4.3 不被视为隐私的信息	51
9.4.4 保护隐私信息的信息	51
9.4.5 使用隐私信息的告知与同意	51
9.4.6 依法律或行政程序的信息披露	52
9.4.7 其他信息披露情形	52
9.5 知识产权	52
9.5.1 HNXACA 自身拥有的知识产权声明	52
9.5.2 HNXACA 使用其他方知识产权的声明	52
9.6 陈述与担保	53
9.6.1 HNXACA 的陈述与担保	53
9.6.2 RA 的陈述与担保	53
9.6.3 用户的陈述与担保	54
9.6.4 依赖方的陈述和担保	54
9.7 担保免责	55
9.8 有限责任	55
9.8 HNXACA 偿付责任限制	55
9.9 用户和依赖方责任	56
9.9.1 用户的赔偿责任情况	56
9.9.2 依赖方的赔偿责任情况	56
9.10 有效期限与终止	56
9.10.1 有效期限	56
9.10.2 终止	57
9.10.3 效力的终止与保留	57
9.11 对参与者的个别通告与沟通	57
9.12 修订	57
9.12.1 修订程序	57
9.12.2 通告机制和期限	57
9.12.3 必须修改 CPS 的情形	58
9.13 争议处理	58
9.14 管辖法律	58
9.15 与适用法律的符合性	58
9.16 一般条款	59
9.16.1 完整协议条款	59
9.16.2 转让条款	59

9.16.3 分割性条款	59
9.16.4 强制执行条款	59
9.16.5 不可抗力条款	59
9.17 其他条款	60
9.17.1 各种规定的冲突	60
9.17.2 安全资料的财产权益	60
9.17.3 损害性资料	60

1 概括性描述

1.1 概述

河南省信息化集团有限公司，又称河南省信息安全电子认证中心（简称“信安 CA、HNXACA”），成立于 2009 年 7 月 6 日，注册资金 3,077 万元人民币。公司先后获得国家密码管理局颁发的《电子认证服务使用密码许可证》、国家工业和信息化部颁发的《电子认证服务许可证》，通过了“国家密码管理局电子政务电子认证服务能力评估”、“国家卫生和计划生育委员会合规性测试”，可以为电子政务及卫生系统提供电子认证服务，是公平、公正、权威的第三方电子认证服务机构。

《河南省信息化集团有限公司电子认证服务业务规则》（以下简称“HNXACA CPS”）是河南省信息化集团有限公司按照《电子签名法》、《电子认证服务管理办法》的要求，规范信安 CA 的电子认证业务的服务、管理，保障认证体系的可靠，维护电子认证的权威性，有效地防范安全风险。明确规定信安 CA 在审核、签发、发布、存档和吊销数字证书等证书生命周期管理以及相关的业务应遵循的各项操作规范。报国家工业和信息化部备案，并在公司官网上进行公示。

信安 CA 严格按照《电子签名法》及《电子认证服务管理办法》等法律法规要求，向用户提供可靠电子认证服务。信安 CA 认证体系内的成员包括有信安 CA（根 CA）、注册机构（业务受理点，即 RA）、数字证书用户、证书依赖方等成员，组成完整的信安 CA 电子认证架构，为用户提供网上安全、可靠的电子身份认证服务。

信安 CA 认证体系内的所有成员都必须严格遵循和执行 HNXACA CPS，并承担相应的责任。

1.2 文档名称与标识

1.2.1 名称

本文档的名称是《河南省信息化集团有限公司电子认证服务业务规则》，简称为 HNXACA CPS，是 HNXACA 在颁发证书过程中所采取的业务操作规则规范。

1.2.2 版本

本 HNXACA CPS 是 HNXACA 发布的最新版本，版本号为 V3.4。

1.3 认证体系的成员

1.3.1 电子认证服务机构

HNXACA 是根据《电子签名法》及《电子认证服务管理办法》规定依法设立的电子认证服务机构，是网上安全电子交易中具有权威性和公正性的可信赖的第三方机构。HNXACA 为网上业务的各参与方签发标识其身份的数字证书，并对数字证书进行更新、吊销等一系列管理。HNXACA 设立安全策略管理委员会、安全管理小组等机构，进行相关管理活动。HNXACA 下设服务中心、及业务受理点（RA），进行业务管理及实施活动。

（1）HNXACA 的根：ROOTCA

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

（2）国家 SM2 根（一级）证书：

CN = ROOTCA

O = NRCAC

C = CN

（3）HNXACA SM2 根（二级）信息：

CN = XACA

OU = HNXACA

O = HeNan Province Information Development Co. Ltd

L = ZhengZhou

S = HeNan

C = CN

HNXACA SM2 根证书的有效期为：2016年 3月 2日 11:35:13——2036年 2月 26日 11:35:13。

1.3.2 注册机构

HNXACA 的注册机构（简称 RA），又称为业务受理点，是 HNXACA 设立或授

权委托设立的数字证书业务受理机构。其业务范围包括：面向用户受理数字证书业务和销售数字证书产品业务。其中受理数字证书业务是指受理用户的证书注册申请、审核用户身份、批准证书申请、证书制作、发放证书、接受和处理证书更新、证书吊销、密钥恢复以及其他需要直接面向用户的业务，其中密钥恢复业务仅由指定受理点开展。销售数字证书产品业务是指销售 HNXACA 的各类数字证书以及数字证书存储介质。

RA 按照 HNXACA 制定的 CPS 及相关业务受理点管理程序运营数字证书代理业务。在代理数字证书业务的运营活动中，应按照 HNXACA 的规定，执行符合政策规定的资费标准，向用户提供统一标准的服务。

HNXACA 各 RA 点挂牌的名称为“数字证书业务受理点”。

1.3.3 订户

订户也称为证书持有者，也称为用户。是指拥有电子认证服务机构签发的有效证书的实体。包括从 HNXACA 处接受证书的任何个人或合法设立的组织。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本 CPS 和相关协议；
- 拥有与接受的证书内公钥所对应的私钥。

1.3.4 依赖方

依赖方包括行为上依赖于 HNXACA 用户的证书及其数字签名的一方，与订户发生业务往来的个人或组织。依赖方可以是、也可以不是一个订户。

1.3.5 其他成员

HNXACA 认证体系在某种专门情况下所声明的其他相关成员。

1.4 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，归为以下三种：

- 个人证书
- 机构证书
- 设备证书

HNXACA 在开展业务时可能为某种对象的证书作特别的命名。

1.4.1 证书性质

证书类型	用户性质	举例
个人证书	各级政务部门的工作人员和参与业务的社会公众，用以代表个体的身份。	如某局职员，参加纳税申报的个人。
机构证书	政务机关和参与业务的企事业单位，代表机构身份。	某部委、某局或参加政府招投标业务的投标企业。
设备证书	系统中的服务器或其他设备，用以代表设备身份的	服务器身份证书、SSL 服务器证书、

1.4.2 禁止的证书应用

各类证书的使用应符合对其用途的限定，如参与方未经 HNXACA 认可或不遵守相关约定，其证书的应用超出限定的应用范围，将不受 HNXACA 的保护。禁止将证书用于违反国家法律、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自行承担。

1.5 策略管理

1.5.1 策略文档管理机构

HNXACA CPS 由 HNXACA 安全策略管理委员会负责起草、注册、维护和更新，版权由 HNXACA 完全拥有。

1.5.2 联系信息

联系地址：河南省郑州市郑东新区明理路祭城南博雅广场 4 号楼 15 层

邮编：450046 网站：www.hnxaca.com

电话：0371-86109777 传真：0371-69176993

电子邮件：service@hnxaca.com

1.5.3 决定 CPS 符合策略的机构

HNXACA 安全策略管理委员会是公司 CPS 策略制定的最高权威机构，审定批准CPS，是决定 CPS 符合策略的机构。

1.5.4 CPS 批准流程

HNXACA 将对 HNXACA CPS 进行严格的版本控制，由 HNXACA 安全策略管理

委员会指定专人负责版本控制及发布。

所有 CPS 相关公告和通知需获得安全策略管理委员会批准后，通过 HNXACA 网站 www.hnxaca.com 进行公布。

根据《电子签名法》及《电子认证服务管理办法》等规定，HNXACA 从对外公布之日起三十日内向国家工业和信息化部备案。

1.6 定义和缩写

1. CA (Certificate Authority)

电子认证服务机构的简称。CA 是网络身份认证的管理机构，是网上安全电子交易中具有权威性和公正性的可信赖的第三方机构。CA 为电子事务的各参与方签发标识其身份的数字证书，并对数字证书进行更新、吊销等一系列管理。

2. RA (Registration Authority)

注册机构的简称。RA 是 CA 认证体系的一个功能组件，负责对数字证书申请进行资格审核，并决定是否同意给该申请者发放数字证书，以及证书更新和吊销工作。

3. KMC (Key Management Center)

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

4. HNXACA

河南省信息化集团有限公司的简称。

5. CPS (Certification Practice Statement)

电子认证业务规则的简称。CPS 详细描述电子认证机构数字证书的发放、吊销、更新、管理的规范，是认证体系各机构运营 CA 系统进行实际工作和运行应严格遵守的各种规范的综合，是数字证书管理、数字证书服务、数字证书应用、数字证书分类、数字证书授权和数字证书责任等政策集合。

6. CRL (Certificate Revocation List)

数字证书吊销列表的简称。CRL 中记录所有在原定失效日期到达之前被吊销的数字证书的序列号，供数字证书使用者在认证对方数字证书时查询使用，由 CA 周期性签发。CRL 通常又被称为数字证书黑名单、数字证书废止列表等。内容通常包含列表签发者、发行日期、下次吊销列表的预定签发日期、被吊销的数

字证书序号，并说明被吊销的时间与理由。

7. 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。

8. 数字证书 (digital certificate)

数字证书是由证书认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。它是用来标志和证明网络通信双方身份的数字信息文件，与机动车驾驶证或日常生活中的身份证相似。在网上进行电子商务等活动时，交易双方需要使用数字证书来表明自己的身份，并使用数字证书来进行有关交易操作。

9. 数字签名 (电子签名 digital signature)

采用密码技术对数据进行运算得到的附加在数据上的签名数据，或是对数据所作的密码变换，用以确认数据来源及其完整性，防止被人（例如接收者）进行篡改或伪造。

10. 金融网上系统 (financial internet system)

金融网上系统是指通过互联网、移动通信网络、其他开放性公众网络或专用网络基础设施向其用户提供各种金融服务的机构。

11. DTS (Digital Time Stamp)

数字时间戳服务的简称。用于向用户提供可信的精确时间源，以证明某个特定时间某个行为或者文档确实存在。时间源采用的是国际标准时间 UTC，通过GPS（全球卫星定位系统）卫星天线接收同步卫星原子钟的精确时间信号。

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吊销列表（CRL）。

13. OID (Object Identifiers)

对象标识符的简称。OID 由国际标准化组织分配和发布，并形成一种层次关系。OID 是一串用点分开的十进制数（例如“1.2.3.4”）。OID 标准的定义来自 ITU-T 推荐 X.208 (ASN.1)，企业（和个人）可以从国际标准化组织申请得到一个根对象标识符，并且可使用它分配根节点下的其他对象标识符。

14. PKI (Public Key Infrastructure)

公开密钥基础设施的简称。PKI 为支持基于证书的公开密钥算法技术的实

现和运作的相关体系、组织、技术、操作和程序的集合。

15. 私钥(Private Key)

是一种不能公开、由持有者秘密保管的数字密钥，用于创建数字签名、解密报文或与相应的公开密钥一起加密机要文件。

16. 公钥(Public Key)

可以公开的数字密钥，用于验证相应的私钥签名的报文，也可以用来加密报文、文件，由相应的私钥解密。

17. 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。

18. URL(UniformResourceLocator)

统一资源位址的简称。URL 是在 Internet 的 www 服务程序上用于指定信息位置的表示方法。

19. X.509

一种由 ITU-T (InternationalTelecommunicationUnion-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。

20. 鉴别

辨别认定证书申请者提交材料真伪的过程。

21. 验证

对证书申请材料和申请者之间的关联性进行确定的活动。

22. 证书主体 (certificate subject)

证书主体是证书公钥对应的实体，它可以是个人、机构、域名等。

23. 订户 (customer)

向 CA 申请证书的实体，包括个人用户和机构订户。

24. 依赖方 (relying party)

使用证书中的数据进行决策的用户或代理。

25. 个人证书 (individual certificate)

以个人用户名义向 CA 申请，用以表示个人身份信息的证书。

26. 机构证书 (organization certificate)

以机构用户名义向 CA 申请，用以表示机构身份信息的证书。

27. 依赖方 (relying party)

使用证书中的数据进行决策的用户或代理。

28. SSL 证书 (SSL (Secure Socket Layer) certificate)

SSL 服务器上需要配置的证书，包含服务器域名或 IP 地址信息，用于对服务器进行身份认证，并在服务器端与用户端之间建立 SSL (Secure Socket Layer, 安全套接层)加密通道，对传送的数据进行加密，并确保数据在传输过程中不会被篡改。

29. 文件证书 (软证书 soft certificate)

指证书及对应私钥以文件形式存储在计算机文件系统中的证书，通常相对于证书及对应私钥保存在智能密码钥匙硬件中的证书而言（又称软证书）。

30. 智能密码钥匙 usb key

智能密码钥匙是一种内置 PKI 密码算法智能芯片、可以安全存储证书私钥和证书、并能进行签名和签名验证所需密码运算功能的硬件设备。

31. 证书更新 (certificate renewal)

证书更新是指在证书所载信息不变的情况下，延长证书的有效期。

32. 证书吊销 (certificate revocation)

证书吊销是指将用户的证书标记为 CA 永远不再信任的状态，并放置于证书吊销列表中供依赖方查询。

33. 证书冻结 (certificate suspension)

证书冻结是指将用户的证书标记为 CA 暂时不信任的状态，并放置于证书吊销列表中供依赖方查询。

34. 证书解冻 (certificate dissuspension)

证书解冻是指将已经冻结的证书标记为 CA 重新信任的状态，并从证书吊销列表中删除其冻结信息供依赖方查询。

35. 证书策略 (certificate policy)

一套指定的规则集，用以指明证书对一个特定团体和（或）具有相同安全需求的应用类型的适用性；或用以指明证书对于具有相同安全需求的某类应用的适用性。

36. 密钥更新 (certificate rekey)

密钥更新是指在不改变证书中用户的其它任何信息的情况下，更换密钥对用户签发一张新证书。

2 信息发布与信息管理

2.1 信息库

HNXACA 信息库是一个对外公开的信息库，它能够保存、取回证书及与证书有关的信息。HNXACA 信息库内容包括但不限于以下内容：证书、CRL，证书状态信息，HNXACA CPS 最新的版本，以及其他由 HNXACA 不定期发布的信息。HNXACA 证书库为信息库的子集，用来存放经 HNXACA 签发的证书和证书吊销列表(CRL)，主要为用户和网络应用提供 HNXACA 证书查询及验证证书状态服务的信息库。用户可登录 HNXACA 网站 (www.hnxaca.com) 查询证书信息或下载证书。HNXACA 信息库不会改变任何从发证机构发出的证书和任何证书吊销的通知，而是准确描述上述内容。

HNXACA 信息库将及时发布包括证书、CPS 修订、证书吊销的通知和其他资料等内容，这些内容保持与 CPS 和有关法律法规一致。

除 HNXACA 授权者外，禁止访问信息库（或其他由 CA 或 RA 维护的数据）中任何被 CPS 和/或 HNXACA 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 CPS 的发布

HNXACA CPS 一经 HNXACA 在网站 (www.hnxaca.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。HNXACA CPS 的发布及更改遵循本规则 1.5.4 的规定。如有需要，可访问 HNXACA 网站 (www.hnxaca.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，如果订户没有要求，HNXACA 默认将该证书副本发布到信息库。HNXACA 定期发布 CRL 以公布在证书有效期内被吊销的数字证书。证书依赖方可在 HNXACA 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 HNXACA 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。

HNXACA 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。

HNXACA 可根据信息系统的需要，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信息系统进行数据同步，将证书信息同步到信息系统中。提供的信息可包括如下信息：业务类型、认证机构身份标识、用户基本信息、用户证书信息等。

HNXACA 可以根据需要，将 CRL 实时发布到指定的信息系统中。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

2.3.1 CPS 的发布时间或频率

HNXACA 将及时发布 CPS 的最新版本，一旦对规则的修改、补充、调整等获得批准，HNXACA 将在网站（www.hnxaca.com）上发布，并将最新的 CPS 发布在 HNXACA 信息库。

HNXACA 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 CPS 的改动，其发布时间和频率将由 HNXACA 独立做出决定。这种发布应该是即时的、高效的，并且是符合国家法律法规要求的。

在 HNXACA 没有发布新的 CPS，或者没有任何形式的公告、通知等形式宣布对 CPS 进行修改、补充、调整或者更新前，当前的 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，HNXACA 自动通过目录服务器或官方网站将该证书副本及 CRL 发布到信息库，发布周期为不大于 24 小时，即在 24 小时内发布最新的 CRL，在紧急的情况下，HNXACA 可自行决定证书和 CRL 的发布时间。

HNXACA 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。用户和依赖方可在 HNXACA 的 LDAP 服务器或指定的信息库上查询、下载数字证书。

2.4 对信息的访问控制

HNXACA 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 HNXACA 工作人员才能编写、修改和删除 HNXACA 在线

发布的信息资料。同时 HNXACA 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用户才有权阅读受 HNXACA 权限控制的信息资料。

对于 HNXACA 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。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

HNXACA 数字证书的命名遵循《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.509 V3 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。

3.1.2 对名称的意义化要求

订户的甄别名(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。

3.1.3 订户的匿名或伪名

在 HNXACA 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。

HNXACA 签发的数字符号X.509 V3标准, 甄别名格式遵守 X.501标准。甄别名的命名规则由 HNXACA 定义。

DN的具体内容由 CN、OU、O、C 等多个部分组成。其中 CN 用来表示用户信息，OU、O用来表示组织机构单位名称、C 用来表示国家。

3.1.5 名称的唯一性

在 HNXACA 证书服务体系中，证书主体名称必须是唯一的。订户的证

书主体甄别名不能相同，必须是唯一的，但对于同一订户，HNXACA 可以用其唯一的主体甄别名为其签发多张证书，当证书申请中出现不同订户存在相同名称时，遵循先申请者优先使用，后申请者增加附加识别信息。寓意区别的原则。

3.1.6 商标的承认、鉴别和角色

HNXACA 签发的证书主体甄别名中不包含商标名。

3.1.7 各类数字证书 CN 的取值方式

各类数字证书 CN 取值方式如下：

证书类型	政务中的类型	CN 取值方式
个人证书	政务部门工作人员	个人姓名（与身份证明文件上标明的主体名称一致）
个人证书	社会公众	个人姓名（与身份证明文件上标明的主体名称一致）
机构证书	政务部门	机构名称（与机构有效证件上标明的一致）
机构证书	企业	机构名称（与机构有效证件上标明的一致）
机构证书	代码签名	机构名称（与机构有效证件上标明的一致）
设备证书	设备	域名、IP 地址或其他实体标识，与盖章申请表上标明的一致

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

HNXACA 为证书申请者提供电子密匙或其他符合要求的密码设备，用于生成和保存密钥对，保证私钥不被泄露，并将此电子密匙安全地传递到用户手中。

HNXACA 也可通过证书请求（如 PKCS #10）中的数字签名来确认证书申请者持有与注册证书对应的私钥。

证书申请者必需依据法律法规获取和使用密码。

3.2.2 机构的身份确认

HNXACA 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。HNXACA 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。HNXACA 采用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 HNXACA 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。

一般需提供以下资料到 HNXACA 或 HNXACA 的 RA 进行身份审核及确认：

1. 申请表

2. 申请机构的如下有效证件的正本或其副本。有效证件的类型如下：

- 组织机构代码证
- 营业执照
- 企业法人营业执照
- 事业机构登记证
- 事业机构法人登记证
- 税务登记证
- 社会团体登记证
- 社会团体法人登记证
- 人民团体登记证
- 人民团体法人登记证
- 政府批文
- 境外机构的有效证件
- 其他有效证件

3. 经办人身份证明原件。有效证件的类型如下：

- 身份证
- 户口本
- 护照
- 回乡证
- 军人身份证明

- 授权委托书
- 其他有效证件

HNXACA 在认为申请人的身份已经通过其他方式确认，则无需提交任何证件。是否需要提交及提交何种证件，HNXACA 将在证书申请表中予以明示。

HNXACA 还可通过在线电子化的方式进行身份确认。CA 机构或授权机构可通过可信任的第三方数据库等手段进行身份核验。

HNXACA 及其授权的注册机构按照规范对申请材料的原件、复印件、或其他电子材料的真实性进行审核，审核批准后，HNXACA 或授权的注册机构按照相关法律法规要求妥善保存订户申请资料，HNXACA 保存的订户申请资料可以是纸质版或电子版。

HNXACA 或 HNXACA 的 RA 的业务受理人员在认为有必要的情况下，采取电话调查、实地考察或其他验证方式（包括第三方平台数据、互联网访问等）鉴定用户身份及其声明的 IP 地址和域名等信息，申请机构有配合业务受理员的调查工作的义务。

3.2.3 个人的身份确认

HNXACA 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。HNXACA 通过查验证明其个人身份的原件，或通过第三方信息数据或服务，或电话访问等 HNXACA 认为恰当的查验方式来确定个人的身份，一般情况下，个人申请者应提供以下资料到 HNXACA 或其 RA 进行身份审核及确认：

1. 申请表。个人若需在证书中标明个人所属机构，其所属机构身份必须通过 HNXACA 的审核，并且其申请表必须由所属机构盖章。

2. 个人身份证明原件。有效证件的类型如下：

- 身份证
- 户口本
- 护照
- 回乡证
- 军人身份证明
- 其他有效证件

3. 如果是属于政府部门中的个人，申请人还需提供属于所在组织（所在部

门)的证明(包括雇佣关系)。

HNXACA 在认为申请人的身份已经通过其他方式确认,则无需提交任何证件。是否需要提交及提交何种证件,HNXACA 将在证书申请表中予以明示。

HNXACA还可通过在线电子化的方式进行身份确认。CA机构或授权机构可通过公安部身份库、电信运营商身份库等手段进行身份核验。

HNXACA及其授权的注册机构按照规范对申请材料的原件、复印件、或其他电子材料的真实性进行审核,审核批准后,HNXACA或授权的注册机构按照相关法律法规要求妥善保存订户申请资料,HNXACA保存的订户申请资料可以是纸质版或电子版。HNXACA 或其 RA 的业务受理人员在认为有必要的情况下,采取第三方信息数据或服务鉴定用户身份,申请人有配合业务受理员的调查工作的义务。

3.2.4 不予验证的用户信息

未在前面所列的,对于不影响用户身份追溯的信息,HNXACA 一般不予验证。

3.2.5 审核认证体系成员身份确认

1. RA 所属单位必须为依法设立的机构,其身份审核依据本文 3.2.2 的要求进行,并由 HNXACA 进行实地的考察后可确认其身份。

RA 的资格由 HNXACA 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 HNXACA 的相关规定。

2. 业务受理人员 HNXACA 的业务受理人员必须是 HNXACA 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 HNXACA 的相关规定。

3.2.6 互操作原则

HNXACA 通过可能存在的国家根 CA 或者通过交叉认证、证书交换中心等,与其他认证中心建立相互认证的关系。如 HNXACA 与其他 CA 进行了的相互认证,将在 HNXACA 的网站中公布。

HNXACA 在进行相互认证时遵循相关法律法规的规定,如果相关法规未列明的要求则采取对等的方式,以降低信任管理等级为标准。

3.3 证书（密钥）更新请求中的身份鉴别

3.3.1 常规密钥更新的标识与鉴别

数字证书用户申请更新数字证书（密钥）时，需要经过身份审核，才能够完成更新的过程。

HNXACA 可以采用以下方式之一来对更新证书中的身份进行鉴别：

（1）用原证书提交合法有效的数字签名的更新申请，则身份审核通过，无需再次进行其他形式的身份审核；

（2）等同采用本文 3.2 身份的初始验证方法。

3.3.2 吊销后密钥更新的识别预报鉴别

不提供证书吊销后的密钥更新。

3.4 证书吊销请求中的身份鉴别

数字证书用户申请吊销数字证书时，需要经过身份审核，才能够完成吊销的过程。

HNXACA 可以采用以下方式之一来对吊销证书中的身份进行鉴别：

（1）用原证书提交合法有效的数字签名的吊销申请，则身份审核通过，无需再次进行其他形式的身份审核；

（2）等同采用本文 3.2 身份的初始验证方法。

4 证书生命周期操作规范

4.1 证书申请

HNXACA 通过 RA 受理实体或者在线服务系统进行的证书申请。证书申请的实体可以是任何个人、机构或其他客观存在的实体，其本人或机构的合法授权代表或实体拥有者都可以为该实体提交证书申请。证书申请人提交的信息必须真实，否则后果由证书申请人承担。HNXACA 为机构的证书申请表格设置经办人栏，该经办人视为获得机构授权办理数字证书相关业务，包括接受数字证书。

HNXACA 数字证书申请流程为：

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

② 按照本文 3.2 身份鉴别要求提交对应实体类型的证书申请表格及相关身份证明资料，到 HNXACA 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

HNXACA 或其 RA 首先按本文 3.2 的条款对证书申请进行身份审核，以鉴别其身份的真实性。

4.2.2 证书申请的接受与拒绝

HNXACA 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，则给予接受该证书申请，并向 HNXACA 提交证书签发请求。

任何不能提供足够的身份证明材料，或被 HNXACA 或其 RA 怀疑提供虚假信息的，或未在约定时限内支付相关费用的，或未满足 HNXACA 其他申请要求条件的，HNXACA 或其 RA 有权拒绝其申请。

4.2.3 处理证书申请的时间

一般情况下，HNXACA 处理证书申请的时间不超出 48 小时，或按双方约定的处理时限。

HNXACA 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。

4.3 证书签发

HNXACA 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。

HNXACA 与 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。

HNXACA 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，HNXACA 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 HNXACA 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。HNXACA 签发证书使用安全的存储介质（如 USB Key）中生成并写入包含用户真实身份的证书，并从技术上保证信息不被篡改。同时用技术和制度保证在证书生成时，签名证书相对应的私钥只留存在安全的存储介质中，CA 不应留存任何私钥备份，用户加密证书，在 CA 归档中保留有对应私钥。

证书签发后，由 RA 作相应的后续处理，包括为用户将证书安装在电子密钥中并进行证书发放，或通知用户自行下载安装。RA 可以采取以下方式告知用户：

- 网站公告或通知；
- 在 RA 受理点面对面告知；
- 电话通知；
- 电子邮件或其他信函通知。

4.4 证书接受

4.4.1 证书的发布

证书签发后，HNXACA 将证书发布到 HNXACA 证书库。

4.4.2 接受证书的方式

根据不同的业务操作流程，以下任何一种情况均视为用户接受数字证书：

1. 经办人在证书领取记录上签字；
2. 用户获取数字证书及其 PIN 码或口令；
3. 用户从网上下载该数字证书；
4. 与用户约定的其他方式。

4.5 密钥对和证书的使用

4.5.1 用户私钥和证书的使用

用户只有接受了数字证书后方能使用证书对应的私钥。用户结合签名证书及加密证书的功能，在允许的应用范围内使用数字证书。用户使用数字证书时必须遵守国家相关法律法规、HNXACA CPS 和签署的协议。

用户必须确保自己的私钥不被他人窃取。如果用户无法确定其私钥为安全的，请及时向 HNXACA 申请吊销私钥对应的数字证书，以免因此造成损失。

用户必须按密钥的用途来使用相对应的证书，否则不被依赖方认可的责任由用户自行承担。

4.5.2 依赖方对他人证书和公钥的使用

证书依赖方获得对方的数字证书和公钥后，可以通过查看数字证书来了解对方的身份，通过公钥验证对方数字签名的真实性。验证证书的有效性包括以下三个方面：

1. 验证该证书为 HNXACA 签发；
2. 检查该证书在有效期内；
3. 查验该证书没有被吊销。

证书依赖方依据 HNXACA 的相关保障措施，确定自己对对方数字证书的信赖程度。

在验证数字签名时，证书依赖方应参照 HNXACA CPS，通过查看或判定证书使用目的和密钥的用途来评估决定是否接收用户的行为，对于不符合证书或密钥用途的证书使用，依赖方可以拒绝接收。

4.6 证书更新

数字证书的有效期限自证书受理之日起算起，以实际缴费年限为准，若数字证书有效期到期后，用户仍需继续使用数字证书且证书中任何用户信息不变的情况下，为用户签发一张有效期延长后的数字证书。

4.6.1 证书更新的情形

1. 证书将要到期或已到期或 HNXACA 其他策略要求原因，且密钥对处于安

全状态并且策略允许继续使用。

2. 用户或其授权代表提出证书的更新申请。
3. HNXACA 的策略要求或相关法律法规引致其他原因。

4.6.2 证书更新请求的处理

处理证书更新请求可以有以下两种方式：

1. 在线更新，只适合于证书未过期且未被吊销的情形。即在证书即将过期前，通过 HNXACA 网站提交更新申请，经过 HNXACA 证实提交更新申请者拥有对应证书的私钥并收到相关款项后，由 HNXACA 签发新的证书。用户需在声明的处理时间之后，凭提交更新申请的证书公钥所对应的私钥下载新的证书。

2. 离线更新，适合所有证书更新情形。即用户或其授权代表提交证书更新申请表和身份证明材料，到 HNXACA 或其 RA 进行证书更新。其身份鉴别方式和处理过程与本文 4.2 的要求相同。

4.6.3 证书更新的签发、发布和用户接受

1. 证书更新的签发与本文 4.3 相同；
2. 证书更新的发布和用户的证书接受与本文 4.4.1、4.4.2 规定相同。

4.7 证书密钥更新

证书密钥更新是指用户生成一对新密钥并申请为新公钥签发新证书，也就是说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. 因私钥泄漏而吊销证书之后；
2. 证书到期且密钥也到期；
3. 用户或其授权代表提出证书密钥的更新申请；
4. HNXACA 的策略要求或相关法律法规引致其他原因。

4.7.2 证书密钥更新请求的审核

证书密钥更新请求的处理应根据用户的实际情况而采用灵活的处理方式，应根据用户业务安全的需求，选择合适的密钥更新时间 and 周期。密钥更新的签发过程与本文 4.6.2 相同。

4.7.3 证书密钥更新的签发、发布和用户接受

1. 证书更新的签发与本文 4.3 相同；
2. 证书更新的发布和用户的证书接受与本文 4.4.1、4.4.2 相同。

4.8 证书变更

证书变更是指证书用户的信息发生变化进行的重新登记和处理。如果涉及证书记载内容的变化，则需要重新制作证书。

4.8.1 证书变更的内容

用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 证书变更请求的审核

用户或其授权代表提交证书变更申请表和身份证明材料，到 HNXACA 或其 RA 进行证书变更。其身份鉴别方式与本文 4.2 的要求相同。如果涉及其证书内容变更的，则需要重新为用户制作新的证书。其处理方式同本文 4.2 的要求，同时吊销原证书（参见本文 4.9）。

HNXACA 或其 RA 在收到证书更新申请后的 5 个工作日内处理完成。通过证书更新申请的予以更新证书，拒绝用户的证书更新申请的，应在 5 个工作日内通知用户并告知其原因。

4.8.3 证书变更的签发、发布和用户接受

1. 证书变更涉及的证书签发与本文 4.3 相同；
2. 证书变更后用户的新证书发布和用户的证书接受与本文 4.4.1、4.4.2 规定相同；
3. 证书变更后因吊销原证书引起的 CRL 签发与发布同本文 4.9.5；
4. 如果证书变更仅涉及非证书记载内容的变化，则 HNXACA 或其 RA 不予发布，除非与用户或依赖方另有约定。

4.9 证书的吊销和挂起

4.9.1 证书吊销的情形

1. 数字证书私钥泄露丢失；

2. 证书中的信息发生重大变更；
3. 用户不希望继续使用数字证书；
4. 单位终止等原因致用户主体不存在的。；
5. 对于下列情形之一，HNXACA 有权主动吊销所签发的证书：
 - a) 用户申请证书时，提供不真实信息；
 - b) 用户未按照规定缴纳数字证书相关费用；
 - c) 证书对应的私钥泄露或出现其他证书的安全性得不到保证的情况；
 - d) 用户不能履行或违反了相关法律、法规和本协议所规定的责任和义务；
 - e) 法律、法规规定的其他情形。

证书的吊销既可以是用户提出申请，也可以是 HNXACA 因为用户的变更事实或违反约定事实而强行吊销。

4.9.2 请求证书吊销的实体

根据不同的情况，证书依赖方、订户、HNXACA 、注册机构等可以提交证书问题报告并请求吊销证书。

4.9.3 吊销请求的流程

1. 在发生证书需吊销的情形时，用户应当立即到证书注册机构申请吊销证书。及时填写证书吊销申请表，并按本文 3.2 的要求携带身份证明材料，遵循 HNXACA 的吊销规定。

2. 如果单位终止等原因致用户主体不存在的，法定责任人应携带相关证明文件及原数字证书，向注册机构请求吊销用户证书。

HNXACA 或其 RA 按本文 3.2 的要求在 24 小时内进行身份审核通过后，在系统中完成证书的吊销操作，用户或相关法定责任人应当承担在证书吊销之前所有使用数字证书而造成的责任。

当 HNXACA 或其 RA 吊销某一证书时，将在完成吊销操作后按其登记的联系方式通知用户。

4.9.4 吊销请求的宽限期

如果发生需要吊销证书的情形时，订户应该实时提出吊销请求，如果确实因为客观原因导致延迟的，这个时间也不能超过 8 小时。如果在宽限期内，因订户未及时提出吊销请求而产生的任何损失和责任，HNXACA 并不承担。

4.9.5 证书挂起的处理

目前 HNXACA 不提供证书挂起服务。一旦提供挂起服务，HNXACA 将会通过网站进行公布。

4.9.6 证书吊销和挂起状态的发布

任何时候证书被吊销，HNXACA 在 24 小时内将该信息发布到 HNXACA 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。

当吊销的证书过期时会被从下次发布的 CRL 中撤出。

在这期间由于证书吊销使证书不可用造成的用户损失由订户负责。

4.9.7 依赖方检查证书状态的要求

依赖方根据应用场合的不同，使用以下两种方式来检查依赖证书的状态：

1. CRL 查询：依赖方从证书列明的 URL 下载 HNXACA 签发的最新 CRL 到本地，从中查询所依赖证书的状态；
2. OCSP 查询：通过 HNXACA 提供的 OCSP 服务，依赖方可以采用 OCSP 协议获得 HNXACA 在线签发的所依赖证书的状态。

4.10 证书状态服务

HNXACA 提供 7×24 小时的证书状态查询服务。

用户和依赖方可以从 HNXACA 的网站或目录服务器下载 CRL 查询证书状态，或使用 HNXACA 或第三方的 OCSP 用户端工具进行在线的证书状态的查询。对非在线用户，可直接在 HNXACA 的网站上下载 CRL 文件，通过此文件可离线查询证书状态。

HNXACA 无法控制 OCSP 的同时在线访问量，因此可能造成网络拥挤而影响响应速度。HNXACA 可为某些应用场合提供定制的 OCSP 服务。

4.11 订购结束

以下两种情况，表明证书订购结束：

1. 证书在有效期内被吊销，并不再更换新的证书；
2. 证书有效期期满后，用户不再进行证书更新或证书密钥更新。与未到期的其他吊销用户对比，其证书不会进入 CRL。

4.12 密钥生成、备份和恢复

4.12.1 密钥的生成和备份

HNXACA 颁发的用户证书中，含有签名用途的密钥对由用户生成或由 HNXACA 提供的电子密匙生成，HNXACA 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密钥管理中心（以下简称 KMC）产生，并在 KMC 备份托管，HNXACA 的密钥管理中心由河南省国家密码管理局进行管理。

4.12.2 密钥的恢复

这里的密钥恢复即指用户的加密密钥对恢复。用户在 KMC 托管的加密密钥对在需要找回情况下可申请密钥恢复业务，其流程如下：

提交密钥恢复申请表，以及本文 3.2 的身份初始验证所述之身份证明材料到 HNXACA 指定的具有开展密钥恢复业务权限的业务受理机构办理。

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 使用用户或 HNXACA 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。

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

HNXACA 机房的选址和建设按照《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。

HNXACA 的主机房根据业务功能划分为公共区、服务区、管理区、核心区，各功能区域对应的级别分别为控制区、限制区、敏感区、机密区，安全等级和要求逐级提高，并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 HNXACA 的规定要求执行。

5.1.2 物理访问

HNXACA 将功能区域按低到高划分为不同的四个安全等级，为公共区、服务区、管理区和核心区，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、智能卡和指纹双因素控制、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。

HNXACA 设置指纹和智能卡双因素门禁系统来提高访问授权的安全性，并在进入管理区和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 HNXACA 安全管理小组授权的工作人员陪同下，并获得 HNXACA 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

HNXACA 系统由两路不同高压下的双路电源提供供电，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），避免电压波动和持续 8 小时不间断电力供应。

HNXACA 系统的空调系统使用专用中央空调，同时备有独立的机房精密空调，

达到机房温度和湿度的控制要求。

HNXACA 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

HNXACA 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，发现水患可以及时报警。

5.1.5 火灾预防和保护

HNXACA 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、邮件、短信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。同时 HNXACA 制定了火灾事故专项应急预案，在 HNXACA 机房受到火灾威胁的时候启动应急预案，确保机房和 CA 系统的安全。

5.1.6 介质存储

HNXACA 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储存柜中，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。HNXACA 对介质的存储地点进行监控，并且只有授权人员才能进入。

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，HNXACA 在它们作废前或保存期满后进行销毁。HNXACA 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

HNXACA 采用异地备份机制，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异地防灾备份，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 入侵侦测报警系统

HNXACA 在 CA 机房内部署了入侵侦测报警系统，并进行安全布防，发生非法入侵会自动报警并通知相关负责人，保护机房场所的安全。

5.2 操作过程控制

5.2.1 可信角色

所有涉及 CA 及其 RA 业务操作和维护管理的人员，可能是 HNXACA 雇员或代理人员、承包人员、顾问等，都属于可信人员。这些可信人员担任的角色包括但不限于以下部分：

- 1 RA 业务操作员
- 2 RA 业务管理员
- 3 RA 超级管理员
- 4 CA 业务操作员
- 5 CA 业务管理员
- 6 CA 超级管理员
- 7 系统管理员
- 8 密钥管理员
- 9 安全管理员
- 10 安全审计员
- 11 用户服务人员

5.2.2 角色要求的人数

HNXACA 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

以下但不限于以下承担任务的角色必须分离开：

1. 证书业务受理；
2. 证书或 CRL 签发；
3. 系统工程与维护；
4. CA 密钥管理；
5. 安全审计。

5.3 人员控制

5.3.1 人员资格要求

HNXACA 在录用担任可信角色的人员之前，除需满足一般的技能和经验要求外，必须按 HNXACA 可信人员背景调查管理的相关操作指南要求，对录用岗位的可信人员进行对应调查级别的背景调查，符合要求方予录用。可信人员背景调查至少包括以下方面：

- 学历、学位、职称
- 过往的就业情况

对于较高可信等级的调查可能还包括社会关系、奖惩记录、犯罪记录、社会保险记录、交通违章记录、财务信贷记录等。

5.3.2 背景调查程序

首先拟录用担任信任角色的人员需同意 HNXACA 作背景调查。HNXACA 采取调阅人事档案、访问过往就读学校和就职单位的人事主管或同事、参阅政府相关部门的个人记录等方式，核实拟录用人所声明和未声明的信息，并作出评估。评估通过后需签署保密协议和就业限制协议，方可录用。

新入职的员工必须经过三个月的观察期，观察期通过后才可独立上岗。

HNXACA 不定期进行可信人员背景调查，以便能够持续验证人员的可信程度和工作能力。

5.3.3 培训要求

HNXACA 为员工提供必要的培训，帮助员工胜任其目前的工作并为将来的发展做准备。HNXACA 根据需要对员工进行职责、岗位、技术、政策、法律和安全

等方面的培训。

HNXACA 根据各岗位要求对员工进行相应的培训，包括但不限于：企业文化、规章制度、岗位职责等基本培训；《电子签名法》及《电子认证服务密码管理办法》、《电子认证服务管理办法》等相关法律法规的培训；HNXACA 的 CPS；HNXACA 的安全原则和机制；HNXACA 的系统运行、维护、安全；HNXACA 的政策、标准、程序；以及岗位技能、行为方式等其他必要的培训。

5.3.4 再培训要求

HNXACA 定期对员工进行再培训，以不断提高员工业务素质 and 综合能力。同时根据 HNXACA 策略调整、系统更新升级或功能增加等情况，对员工进行继续培训，使其更快更好适应新的变化。

5.3.5 工作轮换周期和顺序

对于可替换的角色，HNXACA 将根据业务的安排进行工作轮换，轮换的周期和顺序将视具体的业务情况而定。

5.3.6 对未授权操作的处理

HNXACA 员工所有涉及到业务操作安全的操作均有记录。记录由 HNXACA 系统管理员或安全审计员审查。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，HNXACA 将立即中止该员工进入 HNXACA 证书认证体系各系统。当事人的证书和操作权限即时吊销，所做的未授权操作将立即被吊销失效。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。

5.3.7 独立合约人要求

HNXACA 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和培训和安全规范。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的监督。

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，HNXACA 应该给相关员工提供有关的文档，至少包括 CPS。《公司章程》制度，岗位说明，相关培训资料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

HNXACA 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、吊销，密码设备的启用、停用、转移和吊销。
- 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、、吊销，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。
- 其他安全事件。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

HNXACA 审计人员每月对日志进行一次审查，识别可疑的事件，核实系统和操作人员是否按规定操作，并记录和报告审查的结果。

5.4.3 审计日志的保存期限

对于纸质日志，现场保存至少 1 个月，归档保存期限为 10 年以上，满足本文 5.5.2 要求的档案保存期限。

对于系统自动记录的日志，分在线保存和离线保存，其中在线保存是把日志留在运行的数据库或文件中保存；离线保存则是把数据库或文件中某段时间的日志以文件转储的方式分开保存。在线保存期限为 1 年，离线保存的保存期限为 10 年以上，满足本文 5.5.2 要求的档案保存期限。

5.4.4 审计日志的保护

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

5.4.5 审计日志的备份

HNXACA 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异地，并需要授权才能取阅或恢复。

5.4.6 审计日志的采集

HNXACA 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

HNXACA 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 HNXACA 保留进一步追究责任的权利。

5.4.8 脆弱性评估

HNXACA 不定期对系统进行脆弱性评估，每年不低于1次，包括从内部和外部对系统可能面临的威胁进行评估，根据评估结果，及时调整和系统运行密切相关的安全控制措施，以降低系统运行的风险。

5.5 记录归档

5.5.1 归档记录种类

HNXACA 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、HNXACA 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

HNXACA 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

HNXACA 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

HNXACA 每天对 CA 系统产生的电子档案进行备份。每周进行一次全备份并异地保存；对于纸质档案，则依据使用要求，按及时保存原则分别制定归档流程。

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，禁止在非授权的情况下对档案及其备份进行删除、修改等操作。

5.5.5 记录时间戳的要求

所有记录都在存档时加上具体准确的时间以表明存档时间，系统产生的记录，由系统自动添加时间，但这些时间未使用时间戳技术表明存档时间。

5.5.6 档案采集系统

HNXACA 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 获得和检验归档信息程序

只有在授权的可信人员在受控的情况下才可以看到和获得归档的信息。

5.6 电子认证服务机构密钥更替

HNXACA 使用国家根。国家根的密钥更替遵循国家根的有关规定。在CA根证书到期时，需要更换密钥，且遵循以下原则：

- 在CA证书生命周期结束前停止签发新的下级证书，确保在CA的证书到期时所有下级证书也全部到期；
- 在停止签发新的下级证书后至证书到期后，继续使用CA私钥签发CRL, 直到最后一张下级证书过期；
- 生成和管理CA密钥，建立遵守密钥管理规范；
- 及时发布新的CA证书；
- 确保整个过度过程安全、顺利、不出现信任真空期。

5.7 损害和灾难恢复

5.7.1 HNXACA 遭攻击或发生损害事故时的恢复程序

HNXACA 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。HNXACA 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，HNXACA 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，HNXACA 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。如果需要吊销 CA 证书，会采取以下措施：

- 立即向电子认证服务管理部门汇报，并启动电子认证服务机构密钥更替流程。
- 立即停止使用该私钥签发证书，并吊销所有已经被签发的证书。
- 立即通知依赖方关闭与证书认证服务相关的系统。
- 通知网站、客户端、短信、电话等方式，告知订户。
- 更新CRL和OCSP信息, 供证书订户和依赖方进行查询。
- 机构密钥更替完成后，未受影响的订户重新签发证书。

5.7.4 灾难发生后的业务保持

当现行 CA 运行系统地点发生灾难，致使 CA 系统不能运作时，HNXACA 启动灾难应急处理程序，异地恢复 CA 系统的运行。

HNXACA 在异地保存有用于 CA 系统恢复的最小资源和最新数据，并预选两个备用地点用于灾难恢复。灾难发生后，HNXACA 会暂停业务受理，但证书及状态查询可以在 24 小时内恢复。

HNXACA 每年最少进行一次灾难恢复和业务持续运作的演练，并对演练程序和结果进行记录，所包括的有关主要人员均参与演练。

5.8 CA 或 RA 业务终止

5.8.1 CA 业务终止

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

HNXACA 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主管部门报告。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，向主管部门提出安排其他认证机构承接业务的申请。

无论如何，HNXACA 继续按照本 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，在 HNXACA 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 HNXACA，并通告其所办理证书的用户。HNXACA 将作出妥善的安排，由其他注册机构或新设注册机构承接其业务，尽量减少对 CA 及证书用户的影响。

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 HNXACA 或 HNXACA 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

HNXACA 及其 RA、用户的所有密钥对，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。

HNXACA 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。

用户的签名密钥对由其持有的电子密匙或其他密码设备产生，而加密密钥对由 KMC 的密码设备产生。

6.1.2 私钥的传递

HNXACA 的私钥只能保存在 HNXACA 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。

用户的签名私钥在用户的电子密匙或其他密码设备生成后随其实物通过离线方式传递到用户；而用户的加密私钥在 KMC 产生后，使用用户对应电子密匙或其他密码设备预生成的公钥加密后经过 CA、RA 传递回用户对应的电子密匙或其他密码设备中，保证传递中间环节加密私钥不泄露。

电子密匙或其他密码设备的离线传递，可以是 CA 或 RA 和用户面对面的交递，或采取邮寄等方式发送（如邮递）给用户。

6.1.3 公钥的传递

用户的公钥采用证书签发请求格式（PKCS#10）或其他专门的安全格式通过安全通道传递给 HNXACA 完成证书签发。这些请求的数据通过网络传输是使用国密局许可的通讯协议和算法，保证传输中的数据安全。

6.1.4 电子认证服务机构公钥传输给依赖方

用户证书签发后其公钥再随证书由 HNXACA 发布到 HNXACA 的证书库，证书依赖方可以从 HNXACA 证书库下载该公钥。

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

6.1.5 密钥长度

现行 HNXACA 的根密钥对及其下级 CA SM2 密钥为 256 位的密钥对。

HNXACA 要求用户的密钥对至少为 256 位的 SM2 密钥对或与此强度相当的其他算法密钥对，否则证书申请不予批准。

6.1.6 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，HNXACA 不会专门安排其质量检查。

6.1.7 密钥用途

在 HNXACA 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。

HNXACA 的签名密钥用于签发下级 CA、用户证书和 CRL。

RA 的签名密钥用于确认 RA 所做的审核证书等操作。

用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。用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

HNXACA 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

HNXACA 采用多人控制策略来管理（包括生成、激活、备份、恢复、停止、吊销）CA 的私钥。

HNXACA 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 M 选 N（其中 M 至少为 3，N 至少为 2 但不大于 M）方式进行私钥的分割，即将管理私钥的数据分割成 M 个部分，由密钥管理人员分别持有，并至少需要 N 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

HNXACA 的根和下级CA 的私钥不进行托管，其他的签名私钥也都不进行托管。根据国家相关法规的要求，HNXACA 代用户向 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。

用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

HNXACA 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，HNXACA 不对用户的私钥进行备份。

6.2.5 私钥归档

HNXACA 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 HNXACA 与用户的协议，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

HNXACA 的 CA 私钥可以在密码模块中导出，以实现私钥备份；HNXACA 的 CA，也可以导入到其他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。

CA私钥的导入和导出，必须由多人控制，通过加密机进行加密导出和导入。

对于订户，HNXACA 不提供私钥从密码模块中导出的方法。

6.2.7 私钥在密码模块中的保存

私钥在硬件密码模块中是以密文的形式保存。

6.2.8 私钥的激活

HNXACA 的私钥采用本文 6.2.2 的控制方式进行激活，至少需要半数以上的密钥管理人员同时在场才能完成操作，从技术和制度上保障敏感加密息操作的安全性。

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。

6.2.9 解除私钥激活状态的方法

CA密钥，当密码硬件模块断电或重新初始化时。私钥进入非激活状态，密码管理员至少半数以上人员在场，登录服务器密码机，进行私钥解除操作。

订户解除私钥状态由其自行决定，当每次操作后注销计算机，或者硬件密码模块断电时，私钥就被解除。

6.2.10 私钥的撤销

当CA密钥不再使用，或者与其对应的公钥到期或被吊销后，加密设备必须被清空。根据厂商的规定，按照操作手册对命要进行销毁。同时，所有用于激活私钥的PIN码。IC卡等也必须被清空或销毁。以上操作至少需要半数以上的密钥管理人员共同在场，由操作员负责清空。

特定情况下需采用物理方式毁坏其中的加密卡、硬盘、内存、闪存以及其它可能存在敏感、机密信息的部件。其余部件按一般设备的摧毁方式处理。根ca密钥的管理员卡、操作员卡、备份卡必须同时进行物理销毁。

6.2.11 密码模块的评估

HNXACA 使用国家密码主管部门鉴定并批准使用的密码设备，符合国家有关标准，接受其颁布的各类标准，规范，评估结果等各类要求。

6.3 密钥对的其他管理

6.3.1 公钥归档

HNXACA 和 HNXACA 用户的公钥会随其证书作为 HNXACA 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 HNXACA 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。

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。

HNXACA 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 HNXACA 产生，或是预制的，或是由计算机随机产生

的。HNXACA 要求其业务人员或建议用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；
- 不能包含用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。

HNXACA 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。

用户应自行评估其电子密钥的 PIN 码的泄露情况，建议用户定期更换 PIN 码。

6.5 计算机安全控制

6.5.1 计算机安全性要求

HNXACA 用于运行认证系统和处理数据的生产用计算机由 HNXACA 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。

HNXACA 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。

HNXACA 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。

HNXACA 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。

HNXACA 定期针对网络环境进行风险评估和审计，以检测有否被入侵的危险，尽可能降低来自网络的风险。

HNXACA 在处理废旧设备时，将会清除影响认证业务安全性的信息存储并加以确认。

6.5.2 计算机的安全等级

HNXACA 的计算机系统安全等级基本达到计算机信息系统安全保护等级划分准则（中华人民共和国国家标准 GB/T22239-2019）。

6.6 生命周期技术控制

6.6.1 系统开发控制

HNXACA 的软件设计和开发过程遵循以下原则：

- 1、制定公司内部的升级变更申请流程；
- 2、开发程序必须在开发环境下进行严格的测试成功后，在申请部署于生产环境；
- 3、变更前进行安全性分析。

6.6.2 系统改进控制

HNXACA 认证系统的安全管理控制，严格遵循行业主管部门的有关运行管理规范来进行操作。

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，包括确定认真系统的访问角色、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。

6.6.3 生命周期的安全控制。

HNXACA 认证系统从设计到实现，系统的安全性始终是重点保证的，完全按照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，确保通信数据的安全。在系统安全运行方面，充分考虑人员权限，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 网络安全性控制

HNXACA 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。

CA 与 RA 的功能模块之间的通信采用安全通信协议连接，并采用安全身份认证技术。

HNXACA 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 数字时间戳

HNXACA 系统的所有服务器都与时间服务器的时间同步，保证系统各电子记录需要的时间是准确的。

7 证书、CRL 和 OCSP

7.1 证书

HNXACA 颁发的证书符合《GB/T20518-2006 信息安全技术 公钥基础设施数字证书格式》标准要求，并完全兼容 ITU-TX. 509 和 RFC5280 等国际标准规范，支持大部分标准扩展，并支持自定义扩展项。

7.1.1 版本号

证书版本号为 X. 509 V3。

7.1.2 证书扩展项

HNXACA 证书支持的标准扩展包括：

- 密钥用法 (KeyUsage)
- 证书策略 (CertificatePolicies)
- 主体替换名称 (SubjectAlternativeNames)
- 基本限制 (BasicConstraints)
- 扩展密钥用途 (ExtendedKeyUsage)
- 证书吊销列表分发点 (CRLDistributionPoints)
- 颁发机构密钥标识符 (AuthorityKeyIdentifier)
- 主体密钥标识符 (SubjectKeyIdentifier)

HNXACA 也支持 GB/T 20518 标准及数字证书格式标准中指定的标准扩展，并支持用户自定义私有扩展，可根据用户或应用的要求定制。私有扩展一般情况下为非关键项。

7.1.3 算法 OID

HNXACA 使用 SM3withSM2 算法签发证书，算法 OID 为：

1. 2. 156. 10197. 1. 501。

7.1.4 名称形式

证书主体名称和颁发机构的名称形式遵循本文 3.1 要求，由 DN 表示。另外，HNXACA 颁发的证书支持主体替换名称扩展，在主体替换名称扩展中以包含证书主体的其他相关名称信息，比如电子邮件地址、服务器的 IP 地址或域名等。

7.1.5 证书密钥用法

HNXACA 根据国家主管部门的相关要求，严格规定数字证书的密钥用法。

HNXACA 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。用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。

7.1.6 证书策略 OID

证书策略由证书颁发机构制定并对外发布，并向国际标准化组织申请证书策略对象标识符（OID）以保证互操作性。证书策略 OID 代表证书颁发机构提供服务的相关策略（如 HNXACA CPS）。证书依赖方在接受该证书行为时通过阅读证书策略以帮助确定是否信任该证书。用户必须在阅读并同意证书策略后才到证书颁发机构申请并使用证书。

7.1.7 策略限定符的语法和语义

在 HNXACA 所颁发证书的证书策略扩展项中包含了 CPS 策略限定符，提供了指向 HNXACA CPS 的 URL，从中可以获取 HNXACA 的《河南省信息化集团有限公司电子认证服务业务规则》。

7.2 CRL

HNXACA 发布的 CRL 符合 X.509、RFC5280 标准规范。

7.2.1 版本号

CRL 版本号为 X.509 V2。

7.2.2 CRL 和 CRL 条目扩展项

HNXACA 发布的 CRL 中，包含了以下扩展项：

- 颁发机构密钥标识符（AuthorityKeyIdentifier）
- CRL 编号（CRLNumber）

- DeltaCRL 指示符 (DeltaCRLIndicator, 仅用于 DeltaCRL, 是关键
- 扩展) 如果有明确的被吊销的原因, CRL 条目则会包含被注销的原因扩展 (ReasonCode)。
- 应用如果遇到不认识的关键的 CRL 扩展或者 CRL 条目扩展, 则不能使用该CRL 来验证证书的注销状态。

7.3 OCSP

HNXACA 采用 OCSP 提供在线证书状态查询服务。应用户的要求, HNXACA 可以将 OCSP 服务 URL 写到证书中。OCSP 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, 方便用户及时的获取证书状态信息。

7.3.1 版本号

OCSP 版本号为 V1。

7.3.2 OCSP 扩展项

HNXACA 未使用 OCSP 相关扩展项。如果遇到 OCSP 响应返回 unauthorized 错误码、证书返回 unknown 状态或者不认识的扩展, 则应该使用其他的机制去验证该证书的吊销状态。

8 认证机构审计和其他评估

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

8.1 审计的依据

审计是为了检查和监督 HNXACA 及其下属机构或其他关联机构是否依据《电子签名法》、《电子认证服务管理办法》、《河南省信息化集团有限公司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，是否存在违反其他法律法规以及 HNXACA 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、保障用户权益的目的。

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 HNXACA 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 HNXACA 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

HNXACA 的内部审计周期为每月一次，并且每年进行一次信息安全的风险评估。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、用户反馈异常、重大的系统变更等。

国家电子认证服务主管部门组织的审查为每年一次。

8.4 审计或评估人员的资质

HNXACA 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 HNXACA 的关系

HNXACA 内部审计人员要求与被审计对象无责任关系，为 HNXACA 雇员。

HNXACA 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 HNXACA 雇员，也可以是非 HNXACA 雇员。

外部审计或评估人员应为与 HNXACA 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

HNXACA 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
- 用户服务规范管理
- 综合运营规范（如法规、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，HNXACA 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，HNXACA 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

HNXACA 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，HNXACA 一般不公开审计或评估结果。

9 法律责任和其他业务条款

9.1 费用

9.1.1 证书签发和更新费用

HNXACA 对证书的签发、更新、密钥恢复和管理收取服务费用，费用标准执行国家或地方物价主管部门批准的价格。并根据实际情况，在批准价格之内调整。

9.1.2 证书查询费用

HNXACA 对发布到证书库中的所有证书查询不予收费，但保留对该服务收费的权利

9.1.3 证书状态信息查询费用

HNXACA 对发布到证书库中的 CRL 提供免费下载和使用服务。

HNXACA 的 OCSP 服务和其他定制的证书状态查询服务根据用户的服务协议要求进行收费。

9.1.4 其他服务费用

HNXACA 免费提供本 CPS 和证书业务相关申请表格下载服务。

对于用户要求定制的服务，HNXACA 酌情收取费用。

9.1.5 退款政策

HNXACA 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，HNXACA 均不退还用户任何费用。

在实施证书操作和签发的过程中，HNXACA 遵守严格的操作程序和策略。如果 HNXACA 违背了本 CPS 所规定的责任或其它重大义务，订户可以要求 HNXACA 吊销证书并退款。在 HNXACA 吊销了订户的证书后，HNXACA 将把订户剩余的证书使用费用并扣除相应税费后退还给订户。

此退款策略不限制订户得到其它的赔偿。

完成退款后，订户如果继续使用该证书 HNXACA 将追究其法律责任。

在业务受理过程中，发现申请者提供虚假材料，HNXACA 中止受理，但不予退还已收取的各项费用。

9.2 财务责任

HNXACA 保持足够的财力维持其业务运作和履行应负的责任。HNXACA接受国家电子认证服务主管部门对 HNXACA 财务状况的检查。

9.3 业务信息保密

9.3.1 保密信息的范围

HNXACA 列入保密的信息包括但不限于以下内容：

- 用户的个人信息和（或）机构信息；
- HNXACA 及其代理机构的证书业务处理信息；
- 所有的私钥信息；
- HNXACA 的运行数据和记录，以及保障运行的相关计划；
- HNXACA 与业务代理机构间的商业信息，包括商业计划、销售信息、贸易秘密和在非公开协议下从第三方得到的信息；
- HNXACA 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，HNXACA 没有义务公布或透露用户证书以外的任何信息；
- 其他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 HNXACA 不列入保密范畴：

- 证书所载信息，以及证书状态信息；
- 由 HNXACA 网站或手册公布的信息。包括证书申请流程、证书使用指南、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，HNXACA 保留追究责任的权利。

9.3.3 保护保密信息责任

HNXACA 及其业务代理机构、用户、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。

HNXACA 执行严格的信息保密制度以确保只有经 HNXACA 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 HNXACA 公开或披露其所拥有的机密信息，HNXACA 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，HNXACA 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 HNXACA 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，HNXACA 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，HNXACA 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

HNXACA 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 HNXACA 的服务，就表示已经同意接受 HNXACA 有关隐私保护的声明。

HNXACA 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

订户在申请与享受证书服务过程中所提供的不构成数字证书内容的信息，原则上被视为订户隐私信息。

9.4.3 不被视为隐私的信息

订户再申请于享受证书服务过程中所提供的用来构成数字证书内容的信息，原则上不视为订户隐私信息，（如：公钥证书信息，证书状态信息）。

9.4.4 保护隐私信息的责任

针对因证书服务而获得、接受或知悉的保密信息，各方主体（包括 HNXACA、注册机构、订户、依赖方等）均应承担隐私保护责任。

9.4.5 使用隐私信息的告知与同意

HNXACA 只在其业务范围内使用本文 9.4.2 所列的隐私信息，包括用户身份识别、管理、和服务的目的。这些使用，HNXACA 没有告知用户的义务，也无需得

到用户的同意。

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，HNXACA 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 HNXACA 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，HNXACA 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，HNXACA 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 HNXACA 公开或披露他的隐私信息，HNXACA 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，HNXACA 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 HNXACA 自身拥有的知识产权声明

HNXACA 享有并保留对证书以及 HNXACA 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。

HNXACA 发行的证书及其状态信息，以及 HNXACA 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 HNXACA，这些知识产权包括所有相关的文件、CPS、规范文档和使用手册等。

在没有 HNXACA 预先书面同意的情况下，用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 HNXACA 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 HNXACA 使用其他方知识产权的声明

HNXACA 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，HNXACA 保证都是合法的拥有相应权利。

用户或证书申请人声明并保证其交付给 HNXACA 使用的网络域名、IP 地址、

主体名称及所有其他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、公司名称或其他知识产权等权利，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 HNXACA 的陈述与担保

HNXACA 的担保如下：

- 在批准证书申请和颁发证书中没有 HNXACA 所知的或源自 HNXACA 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 HNXACA 所收到的信息保持一致；
- 除了未经验证的用户信息外，证书中的或证书中合并参考到的所有信息都是准确的；
- 签发给用户的证书符合本 CPS 的所有实质性要求；
- 按本 CPS 的规定，及时吊销证书，并签发 CRL；
- HNXACA 将向用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；
- 其他的陈述与担保参见与用户的服务协议。

9.6.2 RA 的陈述与担保

HNXACA 的 RA 担保如下：

- RA 遵循 HNXACA 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 HNXACA 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；
- 除了未经验证的用户信息外，证书中的或证书中合并参考到的所有信息都是准确的；

- 签发给用户的证书符合本 CPS 的所有实质性要求；
- 按本 CPS 的规定，及时处理证书的吊销申请；其他的陈述与担保参见与用户的服务协议。

9.6.3 用户的陈述与担保

用户的担保如下：

- 用与证书中所含公钥相对应的私钥所进行的每一次签名，都是用户自己的签名，并且在进行签名时，证书是有效的（没有过期或吊销）并已被用户接受；
- 用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；
- 用户在证书申请过程中向 HNXACA 及其 RA 陈述的所有信息是真实的；
- 用户提供给 HNXACA 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，那么用户和代理人两者负有连带责任。用户有责任就代理人所作的任何不实陈述与遗漏，通知 HNXACA 其 RA；
- 用户将按本 CPS 的规定，只将证书用于经过授权的或其他合法的使用目的；
- 用户的证书是终端证书。用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；
- 其他的陈述与担保参见与 HNXACA 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 HNXACA CPS 以及和用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；
- 依赖方在信赖用户的证书前，需收集足够的信息，判断是否 HNXACA 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 CPS 的有关条款。

9.7 担保免责

HNXACA 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），HNXACA 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 HNXACA 签发的数字证书；
- 用户或依赖方没有使用可信赖系统进行证书操作；
- 用户在 HNXACA 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 有限责任

在法律允许的范围内，认证机构订户协议，依赖方协议和其他订户协议限制认证机构承担的责任。责任限制包括排除间接的、特殊意外造成的、偶然的和后续性的损失。

9.8 HNXACA 偿付责任限制

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

HNXACA 及其授权的发证机构，对于一份证书的所有当事人（包括但不限于用户、申请人或依赖方）的合计赔偿责任，不超过该证书的最高赔偿限额，这种

限额可以由 HNXACA 改动。HNXACA 声明的法律赔偿责任之最高限额为该证书相应的服务费用的 10 倍。当事人不能得到赔偿或有异议，可以向主管部门进行反映，责令 HNXACA 履行赔偿责任。

HNXACA 的赔偿责任范围：

- 证书信息与用户提交的资料信息不一致，导致用户或依赖方损失；
- 由于 HNXACA 的原因，导致依赖方或用户自身无法正常验证证书状态而蒙受损失；
- HNXACA 只有在 HNXACA 证书有效期限内承担以上损失或损害赔偿。

9.9 用户和依赖方责任

用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 HNXACA 产生损失，则用户或依赖方应承担赔偿责任。

9.9.1 用户的赔偿责任情况

- 用户申请证书时，因故意、过失或者恶意提供不真实资料，造成 HNXACA 或者其他方遭受损害的；
- 用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 HNXACA 或其 RA，以及使用不安全系统或不当交付他人使用，造成 HNXACA 或者其他方遭受损害的；
- 用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 HNXACA 或者其他方遭受损害的。

9.9.2 依赖方的赔偿责任情况

- 未按 HNXACA CPS 或其他相关协议承担依赖方义务，而造成 HNXACA 或者其他方遭受损害的；
- 未能按 HNXACA CPS 策略识别和信任证书及其行为，而造成 HNXACA 或者其他方遭受损害的；
- 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 HNXACA 或者其他方遭受损害的。

9.10 有效期限与终止

9.10.1 有效期限

HNXACA CPS 自发布之日起正式生效。

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 将自动终止。

9.10.3 效力的终止与保留

HNXACA CPS 一旦终止后，用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

除非参与者之间另有协议约定，HNXACA 在必要的情况下，如主动吊销订户证书，发现订户将证书用于规定外用途及订户其他违反订户协议的行为，可通过适当方式，如电话、电邮、信函、传真等，个别通知订户、依赖方。

9.12 修订

9.12.1 修订程序

HNXACA CPS 由 HNXACA 安全策略管理委员会根据情况进行审查，任何时候 HNXACA 安全策略管理委员会认为有必要时即组织修订。有安全策略管理委员会指定安全管理的人员负责起草CPS初稿形成讨论稿，并征求公司领导和各部门负责人意见。经讨论、修改达成一致意见后形成送审稿。将CPS送审稿提交安全策略管理委员审阅。在取得安全策略管理委员评审意见后，根据评审意见进行修改并提交安全策略管理委员审批，由安全策略管理委员进行CPS文本格式和版本号，形成定稿。修订后的版本经 HNXACA 安全策略管理委员会审批后发布到 HNXACA 网站（www.hnxaca.com），并报送国家工业和信息化部备案。

9.12.2 通告机制和期限

HNXACA 安全策略管理委员会有权作出对 CPS 作任何修改的决定。如果 CPS 的修改没有本质的变化，包括重新排版、勘误、重新表达，联系方式、发布地址变更等，则无需进行个别的通告。

HNXACA CPS 的修改结果在 HNXACA 的网站（www.hnxaca.com）上公布。

所有可能以书面形式提供给用户的 CPS 修订结果，按以下规则发送：

1. 接受者是一个组织，则向其 HNXACA 或其 RA 登记的联系地址发送信

息；

2. 接受者是一个人，则向其申请书上登记的地址发送信息；

3. 这些通知可能用快递或挂号信的方式发送。HNXACA 也可以选择通过电子邮件（E-mail）向用户发送通知，该电子邮件地址在用户申请证书时已注明。

HNXACA CPS 的所有修正、修改和变化在公布后立刻生效。用户如不在修改结果公布之日起七天内作废证书，就视为同意这种修正、修改和变化。

9.12.3 必须修改 CPS 的情形

如果出现下列情况，那么必须对 CPS 进行修改：

- 采用了新的密码体系或技术，并影响现有 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 CPS 的有效性；
- 现有 CPS 出现重要缺陷。

9.13 争议处理

证书用户、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：

- a) 当事人首先通知，根据本《电子认证业务规则》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 HNXACA 或授权机构就本《电子认证业务规则》所产生的任何争议而提起诉讼的，受 HNXACA 工商注册所在地的人民法院管辖。

9.14 管辖法律

HNXACA 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《电子签名法》及《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

HNXACA 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《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》及相关密码技术、产品标准规范等。

若要出口使用于 HNXACA 认证服务的相关产品，可能需要取得相关政府机关的许可。产品出口的当事人必须遵守中国进出口法律和法规。

9.16 一般条款

9.16.1 完整协议条款

HNXACA CPS 及 HNXACA 的相关业务管理办法、国家相关法律法规构成 HNXACA 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 HNXACA 下属 RA 因故吊销，则其管理的相应用户须接受 HNXACA 的业务调配，通过另一 RA 获得相应服务。

若 HNXACA 因政策性原因或其他不可抗力停止服务，HNXACA 之所属用户须按国家规定，接受相应接管 CA 的证书服务条款。

9.16.3 分割性条款

在 HNXACA 的电子认证业务中，因某一原因导致法庭或其他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），用户证书业务相关协议的其他条款仍然生效。

9.16.4 强制执行条款

HNXACA 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他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，HNXACA 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（如用户）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。HNXACA 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用户的服务协议中规定，也可被规定在 HNXACA CPS 中。

9.17 其他条款

HNXACA 对于CPS及相关规定拥有最终解释权。

9.17.1 各种规定的冲突

若 HNXACA CPS 的规定与其他规定、指导方针或协议相互抵触，各参与方必须接受 HNXACA CPS 的约束，除非 HNXACA 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 HNXACA CPS 首次公开发行之前；

该冲突的协议明确的优于 HNXACA 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 HNXACA 的产权所有。

HNXACA CPS：HNXACA CPS 的版权为 HNXACA 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用户（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，公钥为用户（或其雇主或委托人）所有。

HNXACA 的私钥：HNXACA 的私钥是 HNXACA 的财产。这些私钥由 HNXACA 授权分配和使用。

HNXACA 的公钥：HNXACA 的公钥是 HNXACA 的财产。HNXACA 允许使用这些公钥。

9.17.3 损害性资料

证书申请人与用户不能把包含以下言论的任何资料提交给 HNXACA 或其 RA：

1. 毁谤、中伤、不雅、色情、侮辱、迷信、憎恶或种族歧视的言论；

2. 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；

3. 其他违法言论。