河南信安 CA

电子政务电子认证服务业务规则

（版本 2.0）

（生效日期：2019 年 11 月）

河南省信息化发展有限公司

Henan Province Information Development Co.,Ltd

HNXACA电子政务电子认证服务业务规则版本说明

河南省信息化发展有限公司电子政务电子认证服务业务规则如下表所示：

版本	发布日期	备注
1.0	2013年5月30日	依据《电子政务电子认证服务业务规则规范》制定
2.0	2019年11月29日	依据《电子政务电子认证服务业务规则规范》制定

注：河南省信息化发展有限公司已发布最新版本为V2.0

目录

1. 概括性描述

1.1 概述

《河南省信息化发展有限公司电子政务电子认证服务业务规则》（以下简称“HNXACA E-GOV CPS”）是河南省信息化发展有限公司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。以规范河南省信息化发展有限公司（以下简称“HNXACA”）的电子政务电子认证业务的管理，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 HNXACA 在审核、签发、发布、存档和注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。

HNXACA 严格按照《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》、《电子政务电子认证服务业务规则规范》等法律法规要求，向电子政务用户提供电子认证服务。HNXACA 认证体系内的成员包括有 HNXACA（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，组成体系完整的 HNXACA 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。

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

1.2 电子政务电子认证业务范围

1.2.1 数字证书服务

HNXACA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、证书更新和证书注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

HNXACA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HNXACA网站 https://www.hnxaca.com 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 证书用户性质

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电子政务业务的社会公众，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	政务机关和参与电子政务业务的企事业单位，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	电子政务系统中的服务器或其他设备，用以代表设备身份的真实性	服务器身份证书、SSL服务器证书、IPSec VPN 设备证书。

1.2.4 禁止的证书应用

禁止将证书用于违反国家及地方相应法律法规用途。

禁止违反操作规程进行证书应用。

1.3 电子政务电子认证活动参与者

1.3.1 电子政务认证机构

HNXACA 是根据《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》

规定依法设立的电子认证服务机构（简称 CA），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、注销等一系列管理。HNXACA 设立安全管理委员会、安全管理小组等机构，进行相关管理活动。HNXACA 下设服务中心、服务分中心及业务受理点（RA），进行业务管理及实施活动。

HNXACA 的根

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。

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：面向客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、证书注销、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 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，与用户发生业务往来的个人或组织。依赖方可以是、也可以不是一个用户。

1.3.4 其他参与者

HNXACA 认证体系在某种专门情况下所声明的相关其他成员。

1.4 电子政务电子认证策略管理

1.4.1 管理机构

HNXACA E-GOV CPS 由 HNXACA 安全管理委员会负责起草、注册、维护和更新，版权由 HNXACA 完全拥有。

1.4.2 联系方式

总部地址：郑州市平安大道与明理路交叉口西南角博雅广场4号楼15楼

公司总机：0371-86109777

投诉电话：0371-69176991

公司传真：0371-69176993

公司网址：http://www.hnxaca.com

公司邮箱：service@hnxaca.com

1.4.3 批准程序

HNXACA E-GOV CPS 起草后，交由 HNXACA 法律顾问审核通过，安全管理委员会通过后形成决议，在 HNXACA 网站（www.hnxaca.com）发布后，该 CPS 正式生效。

在 HNXACA 证书政策和操作规范做出任何变动之前，HNXACA 安全管理委员会将对提供的变动建议进行研究，做出变更决定。在征询 HNXACA 法律顾问有关法律方面的意见后，形成决议并在 HNXACA 网站(www.hnxaca.com)公布变更后的 HNXACA E-GOV CPS 正式文档，该变更正式生效。

1.5 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、注销等一系列管理。

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，以及证书更新和注销工作。

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

河南省信息化发展有限公司的简称。

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、注销、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）

数字证书注销列表的简称。CRL 中记录所有在原定失效日期到达之前被注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、下次注销列表的预定签发日期、被注销的数字证书序号，并说明被注销的时间与理由。

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

有时直接称为证书。它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，与司机驾照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

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. 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。

11. 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）。

12. 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，并形成一个层次关系。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。

13. PKI(PublicKeyInfrastructure)

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。

14. 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。

15. 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。

16. 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。

17. 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。

18. 电子密匙

一种提供公钥算法计算，可生成密钥对，并对私钥进行保护的密码设备。通常采用 USB 接口通信，故有些地方也称 USBKEY。

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。

1.6 信息发布与管理

1.6.1 认证信息的发布

HNXACA 通过网站公布以下信息：

《电子政务电子认证业务规则》修订以及其他由 HNXACA 不定时发出的信息。

公司网址：http://www.hnxaca.com

本《电子政务电子认证业务规则》发布在 HNXACA 的网站上，供相关方下载、查阅。

本 CA 机构的信息库面向用户及依赖方提供信息服务。提供信息服务包括但不限于以下内容：证书、CPS、CP 以及 HNXACA 不定期发布的信息。

1.6.2 发布的时间与频率

本CA机构的CPS按照8.12.2所述的批准流程，一经发布到HNXACA的网站，即时生效。

1.6.3 信息库访问控制

对于公开发布的CP、CPS和CA证书等公开信息，本CA机构允许公众自行通过网站进行查询和访问。

只有经授权的RA/CA管理员可以查询CA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。

2.1.2 证书版本

HNXACA 颁发的证书符合《电子政务数字证书格式规范》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。

2.1.3 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（Sub jectAlternativelames）

- 基本限制（BasicConstraints）
- 扩展密钥用途（ExtendedkeyUsage）
- 证书注销列表分发点（CRLDistributionPoints）
- 颁发机构密钥标识符（AuthorityKeyIdentifier）
- 主体密钥标识符（SubjectKeyIdentifier）

HNXACA也支持GB/T20518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。

2.2 身份标示与鉴别

2.2.1 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。

2.2.2 组织机构身份鉴别

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
- 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
- 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 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。

2.2.3 个人身份鉴别

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

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 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。

2.2.4 政府部门个人身份鉴别

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。

2.3 密钥更新请求的标识与鉴别

2.3.1 常规密钥更新的标识与鉴别

在密钥更新中，需要经过身份审核，才能够完成更新过程。

HNXACA可以采用以下方式来对更新证书的用户身份进行鉴别：

1）持有有效证书的用户现场进行密钥更新申请，用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，HNXACA使用用户原有公钥验证确认签名来进行用户身份标识和鉴别，也可选择使用与初始身份确认相同的鉴别流程。

2）用户证书已过期时，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，支持持有效证书的用户，用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，HNXACA使用用户原有公钥验证确认签名来进行用户身份标识和鉴别。

2.3.2 注销后密钥更新的标识与鉴别

证书注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。

2.4 注销请求的标识与鉴别

数字证书用户申请注销数字证书时，需要经过身份审核，才能够完成注销的过程。

HNXACA 可以采用以下方式之一来对注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注销申请，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 2.2 身份的初始验证方法。

3. 数字证书服务操作规范

3.1 证书申请

3.1.1 证书申请流程

HNXACA 通过 RA 受理实体的证书申请。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 2.2 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。

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 HNXACAE-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。HNXACA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HNXACAE-GOV CPS的要求准备证书申请材料，并确保申请材料真实准确。
- HNXACA或其授权的注册机构负责接收证书申请者的请求材料，当面对用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HNXACA保留最终的证明材料和确认信息。
- HNXACA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

HNXACA 或其 RA 首先按本文 2.2 的条款对证书申请进行身份审核，以鉴别其身份的真实性。

3.2.2 证书申请批准和拒绝

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。

3.2.3 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。

3.2.4 告知证书申请的结果

证书申请批准后，HNXACA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，HNXACA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

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。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，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。

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指定的载体中并进行证书发放，或通知用户自行下载安装。通常，HNXACA所签发的证书在24小时内生效。

3.3.2 认证机构和注册机构对用户的通告方式

HNXACA通过注册机构，对用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用户。
- 其他认为安全可行的方式通知用户

3.3.3 证书获取方式

用户获取证书有如下方式：

- 由NHXACA或其授权的注册机构将证书安装在指定的载体中，直接交给用户。
- 由HHXANCA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用户。
- 由HNXACA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用户，由用户自行获取。

3.4 证书接受

3.4.1 构成接受证书的行为

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密码信封；
3. 用户从网上下载该数字证书；
4. 与用户约定的其他方式；

3.4.2 认证机构对证书的发布

证书签发后，HNXACA 将证书发布到 HNXACA 证书库。

3.5 密钥对和证书的使用

3.5.1 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 E-GOV 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 申请注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。

3.5.2 信赖方公钥和证书的使用

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. 查验该证书没有被注销。

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 E-GOV 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。

3.6 密钥更新

3.6.1 密钥更新的情形

1. 因私钥泄漏而注销证书之后；
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。

3.6.2 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。

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用户进行查验与鉴别，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用户，在获得HNXACA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HNXACA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，为用户制作新的证书。

3.6.6 通知证书持有者密钥更新

在线自动更新方式，在自动完成更新、给用户颁发新证书时，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，对用户的通告与本文3.3.2规定相同。

3.6.7 构成接受密钥更新的行为

密钥更新后用户的证书接受与本文3.4.1规定相同。

3.6.8 认证机构对密钥更新的发布

密钥更新的发布与本文3.4.2规定相同。

3.7 证书变更

3.7.1 证书变更的情形

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、电子邮件、联系电话等。

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HNXACA的注册机构提交证书变更申请信息。

3.7.5 通知证书持有者证书变更

证书变更对用户的通知同3.3.2。

新证书签发后原证书将被注销，24小时内通过CRL发布。

3.7.6 构成接受证书变更的行为

密钥更新后用户的证书接受与本文3.4.1规定相同。

3.7.7 认证机构对证书变更的发布

变更证书的发布同3.4.2。

3.8 证书注销

3.8.1 证书注销的情形

1. 政务机构的证书用户工作性质发生变化；

2. 政务机构的证书用户受到国家法律制裁；

3. 证书用户提供的信息不真实；

4. 证书用户没有或无法履行有关规定和义务；

5. HNXACA、HNXACA RA 或最终证书用户有理由相信或强烈怀疑一个证书用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匙丢失；

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. 用户或其授权代表提出证书注销申请；

13. 用户违反 HNXACACPS 或签订的相关证书协议；

14. 其他情况。例如因法律或政策等要求 HNXACA 进行临时或永久性的证书注销措施。

证书的注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注销。

3.8.2 可以发起请求注销证书的实体

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

3.8.3 证书注销的申请

证书注销的申请与本文3.1相同。

3.8.4 证书注销的鉴别

证书注销的鉴别与本文3.2相同。

3.8.5 证书注销受理方式

用户可以向HNXACA及其授权的注册机构提交证书注销申请信息。

3.8.6 认证机构处理注销请求的时限

用户提交的注销申请信息，经HNXACA经过鉴别审核，确认符合条件， HNXACA将在24小时内注销证书并发布到证书注销列表。

3.8.7 通知证书持有者证书注销

证书注销对用户的通知同3.3.2。

3.8.8 构成接受证书注销的行为

HNXACA 通知用户证书注销，或用户未在提交注销请求之后的 24 小时内明确对已提交的注销请求提出异议，即视为用户接受证书注销。

3.8.9 认证机构对证书注销的发布

任何时候证书被注销，HNXACA 在 4 小时内将该信息发布到 HNXACA 信息库，并重新签发 CRL。包含该注销或冻结证书状态的 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。

3.8.10 CRL 发布频率

HNXACA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

证书从注销到发布到CRL上的滞后时间不超过24小时。

HNXACA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

HNXACA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

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 客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。

3.9 密钥生成、备份与恢复

3.9.1 证书持有者密钥恢复

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 2.2 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。

3.9.2 问责取证密钥恢复

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）用户密钥恢复：当用户的密钥损坏或丢失后，某些密文数据将无法还原，此时用户可申请密钥恢复。用户向HNXACA或其授权的注册机构申请，经本文2.2身份验证所述身份证明材料鉴别验证审核后，通过HNXACA向密钥管理基础设施请求；密钥恢复模块接受用户的恢复请求，恢复用户的密钥并下载于用户证书载体中。

2）司法取证密钥恢复：司法取证人员向HNXACA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

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

1）HNXACA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

HNXACA 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/T0018的要求。客户端证书介质的底层应用接口符合GM/T0016和GM/T0017的要求。

用户应遵循上述规范以及HNXACA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，造成损失的由用户自行承担。

4.2.2 密码模块安全技术接口

HNXACA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/T0028和GM/T0054的要求。

4.2.3 通用密码服务接口

HNXACA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/T0019的要求。

4.3 集成内容

HNXACA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

HNXACA向应用集成服务用户提供相应的信息服务。

4.4.1 证书信息服务

HNXACA可向用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。

4.4.2 CRL 信息服务

HNXACA 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

HNXACA向用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

HNXACA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 信息服务方式

4.5.1 证书信息同步服务

HNXACA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，HNXACA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。用户也可通过HNXACA信息库获取其相关证书信息。

4.5.2 CRL 信息同步服务

HNXACA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，HNXACA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。用户也可通过HNXACA信息库获取CRL发布信息。

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

4.5.3 服务支持信息服务

HNXACA通过WEB网站等面向电子政务用户发布如下信息：

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。

4.5.4 决策支持信息服务

HNXACA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

HNXACA 将提供面向证书用户和面向应用提供方的服务支持。

5.1.1 面向证书持有者的服务支持

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：为用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。

5.1.2 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。

5.2 服务方式

5.2.1 座席服务

HNXACA 设置有服务热线。热线坐席根据用户的问题请求，协助用户处理。

5.2.2 在线服务

HNXACA 通过以下方式为电子政务证书用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

5.2.3 现场服务

根据服务协议的约定，由 HNXACA 技术工程师和客户服务人员上门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

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

5.2.5 投诉受理

向用户公布投诉电话和传真，并通过 WEB 网站等方式，收集和受理用户投诉，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用户。

5.2.6 培训

HNXACA 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。

5.3 服务质量

HNXACA 的坐席服务、在线服务、现场服务时间做到充分满足用户的需要。服务时间满足 5 天×8 小时。视双方服务协议的约定，可提供延长服务时间。

HNXACA 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。

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

HNXACA 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。

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。

6.1.2 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。

6.1.3 电力和空调

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。

6.1.4 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。

6.1.5 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。

6.1.6 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。

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，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。

6.1.8 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同城异地定时备份，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

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，保护机房场所的安全。

6.2 操作过程控制

6.2.1 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. 客户服务人员

6.2.2 角色的识别与鉴别

所有在HNXACA的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡和指纹识别，进入系统需要使用数字证书进行身份鉴别。CA机构将独立完整地记录其操作行为。

6.2.3 角色职责分离设置

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；

6.3 人员控制

6.3.1 可信人员要求

HNXACA 的所有员工须签订保密协议。录用可信角色的人员，必须具备相应的教育背景、工作资格、从业经历等条件，必须能够提交相应的证明文件。

A、HNXACA 认证业务系统的各类操作人员，必须具备可信、工作热情高的特点，没有影响本职工作的其他兼职行为，没有在认证业务操作上的不尽职、不负责的经历，没有违法乱纪的不良记录。

B、系统操作人员，必须具备认证系统的相关作业经验，或者通过 HNXACA 相关的培训，才能担任。

C、管理人员，必须具备认证操作的实务经验和多年的系统管理运营经验。

6.3.2 可信人员背景审查

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。

首先拟录用担任信任角色的人员需同意 HNXACA 作职前背景调查。可信人员背景调查至少包括以下方面：

A.身份信息，教育背景，职称与任职资格，工作经历，社会关系等基本调查；

B.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、个人征信记录等。

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，必要时，HNXACA 可与有关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，以核实拟录用人所声明和未声明的信息，并作出评估。

HNXACA 员工需要有 3 个月的考察期，关键和核心部位的员工通过录用考察期后，还需要额外期限的考察。根据考察的结果安排相应的工作或者不予录用并且剥离岗位。

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

6.3.3 人员培训及再培训

HNXACA 建立培训制度，明确培训需求、计划、实施、评估、反馈等管理办法，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 根据各岗位要求对员工进行进行职责、岗位、技术、政策、法律和安全等方面的培训，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。关键岗位需进行保密制度等相关培训，加强日常思想教育。

在培训实施过程中，人力资源部需要派出专人对培训进行记录、评估，结合培训评估效果和培训考核的反馈情况进行相关人员的改进规划，完善培训档案，以不断推进培训工作的深入。

HNXACA 定期对员工进行再培训，以不断提高员工业务素质和综合能力。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。

A. 对于公司安全管理策略，应该每年至少进行一次培训；

B.认证系统运营相关的人员，每年至少进行一次相关技能和知识培训；

C.对于认证系统的升级、新的系统的使用、PKI/CA 和密码技术的进步等，都需要根据情况安排相应的培训。

6.3.4 违规行为处罚

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。

6.3.5 外包服务人员及要求

对于提供第三方服务的人员，包括顾问、系统和设备维护人员、外部技术支持人员等，如果其参与的工作属于可信角色范畴，那么其所需的安全要求和HNXACA员工是一致的。除了必须就工作内容签署保密协议以外，该服务人员必须在HNXACA专人全程监督和陪同下从事相关工作。同时还需要对其进行必要的知识培训和安全规范培训，使其能够严格遵守相关规范。

6.3.6 提供给员工的文档

为了使认证系统的运营持续正常安全的运行，HNXACA 应该给员工提供有关的文档，至少包括：HNXACA 的 CPS，公司规章制度，岗位清单和职责说明，相关培训资料，岗位相关的文档资料以及相关安全管理规范等。

6.4 审计日志程序

6.4.1 审计日志定义

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、注销，密码设备的启用、停用、转移和注销。
- 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、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。

6.4.2 审计日志安全检查与风险评估

审计人员对日志进行日常审计，如发现引起安全事故的事件或可能的隐患，将写入审计报告。HNXACA 安全管理小组将每月对审计报告进行评审，确定需要改进的安全措施。同时，HNXACA 每年进行一次信息安全的风险评估。

6.4.3 审计日志记录要求

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

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。

HNXACA定期对纸质日志实施归档，对电子日志实施备份。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。

6.4.4 审计日志处理或归档周期

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。

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。

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。

6.4.5 审计日志检测系统

HNXACA建立证书登录访问时的鉴权检测，保证非授权的访问能够被发现和被记录。

6.5 记录归档要求

6.5.1 记录归档的保存期限

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。

6.5.2 记录归档的保护措施

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。

6.5.3 记录归档的备份程序

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。

6.5.4 记录归档收集系统

HNXACA 的记录归档为专人专岗操作，做好档案的保存归档工作。

6.5.5 记录归档检验机制

HNXACA 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

6.6 认证机构密钥更替

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

密钥对已经被泄漏、被窃取、被篡改或者其他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。

6.7 数据备份

6.7.1 数据备份计划

HNXACA每天定时将系统数据传输至异地进行备份。

6.7.2 异地备份中心

HNXACA采用同城异地备份，在郑州市郑花路设置异地备份中心，用于容灾系统应急恢复。

6.8 损害与灾难恢复

6.8.1 事件和损害的列表

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。

6.8.2 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。

6.8.3 实体私钥损害处理程序

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HNXACA 网站或其他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；

6.8.4 灾难后的业务连续性能力

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。

6.8.5 业务连续性计划

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。

6.9 认证机构或注册机构的终止

因各种原因，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，HNXACA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。

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

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 私钥传送给用户

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它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它密码设备中，HNXACA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和用户面对面的交递，或采取数字信封保护方式发送给用户。

7.1.3 公钥传送给证书签发机构

用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HNXACA，由HNXACA完成证书签发。

7.1.4 认证机构公钥传送给依赖方

HNXACA 的公钥随 HNXACA 根证书发布到 HNXACA 信息库供用户和依赖方下载。

7.1.5 密钥的算法

HNXACA 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

HNXACA 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，HNXACA 不会专门安排其质量检查。

7.1.7 密钥使用目的

在HNXACA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。

HNXACA的签名密钥可用于签发下级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。

7.2 私钥保护和密码模块工程控制

7.2.1 在 CA 私钥保护方面的要求

HNXACA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。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。

7.2.2 用户私钥保护方面的要求

用户的签名密钥对由用户掌握的密码设备生成和管理，为用户专有。

用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

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目录服务器或数据库中，并在其失效后仍会在HNXACA系统中保存至少5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。

HNXACA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

HNXACA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

HNXACA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，HNXACA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

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

整个系统从设计到实现，系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计，使用的算法和密码设备均通过主管部门鉴定，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。

7.6.1 CA 系统运行管理

在系统安全运行方面，充分考虑了系统备份，密钥恢复等安全运行措施，整个系统安全可靠。

7.6.2 CA 系统访问管理

在访问控制管理方面，采用了人员权限分离，确保在授权范围内进行访问。

7.6.3 CA 系统的开发和维护

HNXACA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。HNXACA要求其内部或外包的软件开发项目符合ISO9001：2016质量要求并遵守国家的法规和签署的项目保密条款。

HNXACA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

系统网络安全的主要目标是保障网络基础设施、主机系统、应用系统及数据库运行的安全。CA机构采取防火墙、入侵防御、漏洞扫描等安全防护措施。

7.8 时间戳

HNXACA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. 法律责任和其他业务条款

8.1 费用

8.1.1 免费或收费策略

HNXACA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HNXACA网站上予以公布。

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

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

8.1.2 证书签发和密钥更新费用

HNXACA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 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。对于客户要求定制的服务，HNXACA 酌情收取费用。

8.2 财务责任

8.2.1 责任担保范围

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。

8.2.2 责任赔付声明

当因不遵守操作规程而造成的 RA 身份审核不当或因 HNXACA 密钥泄露而造成的用户或依赖方不应承受的损失，HNXACA 根据 CPS 相关条款和国家相关法规进行赔付。

8.3 业务信息保密

8.3.1 保密信息范围

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。

8.3.2 不属于保密的信息

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。

8.3.3 保护保密信息的责任

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 8.3.1 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。

8.4 个人隐私保密

8.4.1 保护隐私的责任

HNXACA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HNXACA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

HNXACA只在其业务范围内使用用户隐私信息，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。

8.4.3 依法律或行政程序的隐私信息的使用

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用户隐私信息时，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。

8.4.4 不被视为隐私的信息

所有在证书、CRL 载明的用户信息不被视为隐私信息。

8.5 知识产权

8.5.1 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。

8.5.2HNXACA 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。

8.6 陈述与担保

8.6.1 认证机构的陈述与担保

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，及时注销或冻结证书，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。

8.6.2 注册机构的陈述与担保

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，及时处理证书的注销或冻结申请；
- 其他的陈述与担保参见与用户的服务协议。

8.6.3 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、被冻结或注销）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。

8.6.4 依赖方的陈述与担保

依赖方的担保如下：

- 依赖方保证熟悉 HNXACA E-GOV 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，判明是否 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。

8.7 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。

8.8 偿付责任限制

HNXACA 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，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。

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。

8.9 赔偿责任

8.9.1 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 或其他方遭受损害的。

8.9.2 依赖方的赔偿责任情况

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

HNXACA E-GOV 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。

8.10.2 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。

8.10.3 效力的终止与保留

HNXACA E-GOV 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。

8.11 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，否则各参与者之间必须采用书面的的方式（包括有数字签名的电子文书）进行通告和沟通。

信息发送者应确保信息被对方所接收，并能够理解。

8.12 修订

8.12.1 修订程序

HNXACA E-GOV CPS 由 HNXACA 安全管理委员会根据情况进行审查，任何时候 HNXACA 安全管理委员会认为有必要时即组织修订。修订后的版本经 HNXACA 安全管理委员会审批后

发布到 HNXACA 网站（www.hnxaca.com），并报送国家密码管理局备案。

8.12.2 通知机制和期限

HNXACA 安全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 E-GOV 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，则向其在 HNXACA 或其 RA 登记的联系地址发送信息；
2. 接受者是个人，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 E-GOV 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。

8.12.3 必须修改业务规则的情形

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。

8.13 争议处理

如果 HNXACA 与合作机构之间或与用户、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，均提请郑州市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。

8.14 管辖法律

HNXACA 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

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《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。

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。

8.16 一般条款

8.16.1 完整协议条款

HNXACA E-GOV 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。

8.16.2 转让条款

若 HNXACA 下属 RA 因故注销，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。

8.16.3 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。

8.16.4 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。

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；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 E-GOV CPS 中。

8.17 其他条款

HNXCA 对本 CPS 具有最终解释权。