网证通
NET CA

认证业务声明

V3.0版

www.cnca.net

广东省电子商务认证有限公司

Guangdong Electronic Certification Authority

第1章　概括性描述

1.1 概述

为了规范广东省电子商务认证有限公司（以下简称“NETCA”[1]）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，NETCA 制订了《广东省电子商务认证有限公司认证业务声明》（以下简称《NETCA CPS），明确规定 NETCA 在审批、签发、发布和撤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。

NETCA 认证体系内的成员包括有 NETCA（根 CA）、注册机构（业务受理点，即 RA）、数字证书订户、证书依赖方等成员，组成体系完整的 NETCA 电子认证架构，为订户提供互联网上的安全可靠的电子身份认证服务。

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

1.2 文档名称与标识

《广东省电子商务认证有限公司认证业务声明》是本证书认证机构在颁发证书过程中所采取的业务实践的声明，亦即为本公司的 CPS，也可称为本公司的电子认证业务操作规范。

1.3 认证体系的成员

1.3.1 NETCA

NETCA 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、撤销等一系列管理。NETCA 下设安全管理小组等机构，进行相关管理活动。

[1] NETCA 在表示机构为“广东省电子商务认证有限公司”简称，在表示产品和服务时为品牌名称。“网证通”与“NETCA”具有相同的含义。

1.3.2 NETCA 的根

NETCA ROOTCA 是广东省电子商务认证有限公司电子认证系统的根的名称，称为 NETCA 的根。

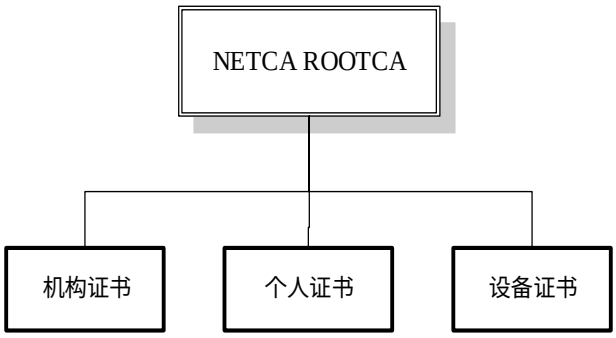

图 1-1NETCA 体系结构图

1.3.3 数字证书业务受理点

数字证书业务受理点（RA ，Registration Authority）为本公司的证书注册机构，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。其中数字证书业务是指受理订户的证书注册申请、审核订户身份、批准证书申请、证书制作、发放证书、接受和处理证书更新、证书撤销，以及其他需要直接面向订户的业务。销售数字证书产品业务是指销售 NETCA 的各类数字证书以及数字证书存储介质。

RA 应按照 NETCA 制定的 CPS 及《广东省电子商务认证有限公司 RA 管理办法》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 NETCA 的规定，使用统一的品牌和标志，执行符合政策规定的资费标准，向订户提供统一标准的服务。

1.3.4 订户

NETCA 的即从 NETCA 接收证书的实体，包括从 NETCA 处接收证书的公众成员、应用系统的使用者、拥有电子商务、电子政务等类网站或系统的组织、组织的雇员等。

1.3.5 依赖方

NETCA 数字证书依赖方的包括行为上依赖于 NETCA 订户的证书及其电子签名的一方，与订户发生业务往来的个人或组织。依赖方可以是、也可以不是一个给定 PKI 的订户。

1.3.6 其他成员

NETCA 认证体系在某种专门情况下所声明的相关其他成员。

1.4 证书的适用范围

1.4.1 正当的证书应用

证书类型	订户性质	适用范围
个人证书	社会自然人 政府、企业、事业机构或其下属部门所属人员	社会自然人或政府、企业、事业机构或其下属部门所属人员在电子事务处理过程中，代表其身份，行使电子签名
机构证书	政府、企业、事业机构或其下属部门	政府、企业、事业机构或其下属部门在电子事务处理过程中，代表其身份，行使电子签名
设备证书	政府、企业、事业机构或其下属部门所属的硬件设备	政府、企业、事业机构或其下属部门所属的在电子事务处理过程代表其硬件设备身份

1.4.2 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。

1.5 策略管理

1.5.1 管理组织

本 CPS 由广东省电子商务认证有限公司认证策略管理委员会负责起草、注册、维护和更新，版权由广东省电子商务认证有限公司完全拥有。

1.5.2 联系信息

TEL：800-830-1330

E-Mail：service@cnca.net

1.5.3 CPS 批准流程

《NETCA CPS》起草后，交由 NETCA 律师审核通过，认证策略管理委员会通过后形成决议，该 CPS 正式生效。在 NETCA 证书政策和操作规范做出任何变动之前，NETCA 认证策略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 NETCA 律师有关法律方面的意见后，形成决议。

NETCA 将在决议形成后，在 NETCA 网站(www.cnca.net)公布变更后的《NETCA CPS》正式文档。

1.5.4 CPS 的发布

NETCA 将对《NETCA CPS》进行严格的版本控制，由 NETCA 认证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认证策略管理委员会批准，方能在 NETCA 网站上公布（www.cnca.net）。

1.6 定义和缩写

1. ASN.1

ASN.1，即抽象符号标记，规定了丰富的数据类型，传输或保存的信息总属于某种特定的数类型。如整型、实型、布尔型、可见字符串型，二进制字符串型，结构类型、集合类型等。

2. CA（Certificate Authority）

认证中心的英文简称。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、撤销等一系列管理。

3. Certification（认证）

不同实体在进行网上交易之前，通过可信赖的、中立的第三方（如 CA 认证

中心）对身份进行审核，并由第三方出具证明证实其身份的可靠性和合法性的过程。

4. CNCA

广东省电子商务认证有限公司的另一个域名标识。

5. CP

Certificate Policy，证书策略，是一套命名的规则集，用以指明证书对一个特定团体和（或者）具有相同安全需求的应用类型的适用性。例如，一个特定的 CP 可以指明某类证书适用于鉴别从事企业到企业（B-to-B）交易活动的参与方，针对给定价格范围内的产品和服务。

6. CPS (Certification Practice Statement)

认证业务声明的英文简称。CPS 详细描述 NETCA 数字证书的发放、撤销、更新、管理的规范，是 NETCA 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。

7. CRL (Certificate Revocation List)

数字证书撤销列表的英文简称。CRL 中记录所有在原定失效日期到达之前被撤销的数字证书的订户数字证书序列号，供数字证书使用者在认证对方数字证书时查询使用。CRL 通常又被称为数字证书黑名单。内容通常还包含列表发行人的姓名、发行日期、下次撤销列表的预定发行日期、遭更新或撤销的数字证书序号，并说明遭更新或撤销的时间与理由。声明了主体的名字或签发中心的身份，确定签名者的身份，表明了数字证书的操作时限，还包括数字证书的序列号。

8. Digital Certificate（数字证书 ）

数字证书又称为数字标识 (Digital ID)。它提供了一种在 Internet 上身份验证的方式，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。通俗地讲，数字证书就是个人或机构在 Internet 上的身份证。

9. Digital Signature（数字签名）

是利用公开密钥算法等方法保证信息传输过程中信息的完整和提供信息发送者的身份认证和不可抵赖性的一种技术。

10. DTS (Digital Time Stamp)

即数字时间戳服务，向订户提供可信的精确时间源，以证明某个特定时间某个交易或者文档确实存在。时间服务器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. Electronic Commerce（电子商务）

指利用电子方式，通过数字化的通信网络和计算机设备，完成事务活动和交易活动中信息存储、传递、发布、查询、数据统计、支付等过程。

12. FTP

File Transfer Protocol 文件传输协议。

13. GMT

Greenwich Mean Time 格林威治标准时间。

14. HASH（哈希）函数

HASH（哈希）函数提供了这样一种计算过程：输入一个长度不固定的字符串，返回一串定长字符串，又称 HASH 值。单向 HASH 函数用于产生信息摘要。最为著名的 HASH 函数如 SHA。

15. HTTP

Hypertext Transfer Protocol 超文本传输协议。

16. HTTPS

Hypertext Transfer Protocol with SSL 采用 SSL 的超文本传输协议。

17. KMC

密钥管理中心。

18. LDAP（Lightweight Directory Access Protocol）

即轻量级目录访问协议，用于查询、下载数字证书以及数字证书撤销列表

（CRL）。

19. Message digest（信息摘要）

信息摘要简要地描述了一份较长的信息或文件，它可以被看作一份长文件“数字指纹”。信息摘要用于创建数字签名，对于特定的文件而言，信息摘要是唯一的。

信息摘要可以被公开，它不会透露相应文件的任何内容，这在数字时间戳应用中是极为重要的。通过使用 HASH 函数，可以对一份文件加上时间戳而不会将文件的内容暴露给任何人知道。

20. NETCA

广东省电子商务认证有限公司的简称，来自于自有品牌“网证通”的英文名称。

21. OCSP (Online Certificate Status Protocol)

即在线查询数字证书状态协议，用于支持实时查询数字证书状态。

22. PIN

Personal Identification Number 个人识别号。

23. PKI

Public Key Infrastructure 公开密钥基础架构。

24. Private Key（私人密钥，简称“私钥”）

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。

25. Public Key（公开密钥，简称“公钥”）

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

26. RA（Registration Authority）

注册中心的英文简称。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，承担因审核错误

而引起的一切后果。

27. Relying party（依赖方）

证书的接收者，他依赖于该证书和（或）可通过该证书所验证的数字签名。

28. Relying party agreement（依赖方协议）

证书认证机构与依赖方所签署的协议，通常规定了在验证数字签名或其他使用证书的过程中有关方所拥有的权利和义务。

29. RSA 算法

RSA 是由 Rivest、 Shamir 及 Adelman 所发明的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。

30. S/MIME (Secure/ Multipurpose Internet Mail Extensions)

安全多用途网络信件扩展格式，是 Internet 中用来发送安全电子邮件的协议。为了使用安全电子邮件——S/MIME，客户端必须使用支持 S/MIME 功能的电子邮件程序，例如 IE Outlook Express 和 Netscape Messenger。

31. SSL (Secure Sockets Layer)

即安全套接层协议，是一种由 Netscape 公司设计，用来进行 Internet 网上保密通信的协议。SSL 协议向 TCP/IP 的客户/服务器应用程序提供客户端和服务器的鉴别、数据完整性和信息机密性等，主要用在网络浏览器和网络服务器之间的通信中唯一资源位址

32. Subscriber（证书持有者）

亦称为订户，直接颁发给一张证书的证书主体。

33. TCP/IP

TCP（Tranform Control Protocol）是传输控制协议，IP（Internet Protocol）是网络协议，TCP/IP 是支持 Internet 通信的协议集。

34. UPS

Uninterrupted Power System 的缩写，不间断电源系统。

35. URL

Uniform Resource Locator ，即唯一资源位址。

36. 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。

37. 个人数字证书

个人数字证书是广东省电子商务认证有限公司专门为个人订户提供的数字证书，以帮助个人订户在网络上表明身份、进行安全事务处理和安全交易操作。具体应用如：发送安全电子邮件、访问安全站点、网上招标、网上签约、网上购物、网上公文安全传送等网上的安全电子事务处理。

我公司需要对该类型数字证书的申请者进行身份审核。

38. 机构数字证书

机构数字证书是广东省电子商务认证有限公司专门为机构或机构中的工作人员提供的数字证书，以帮助机构在进行公务或商业活动时，建立一个虚拟环境中的信任度。机构数字证书主要是用于机构安全电子事务处理。具体应用如：网上公文传送、网上采购、网上签约、网上招标投标、网上办公系统等。

我公司需要对该类型数字证书的申请者进行身份审核。

39. 设备数字证书

设备数字证书是签发给机构的设备，与互联网中的设备名相对应，用来证明设备的真实身份，加强信息数据安全。

我公司需要对该类型数字证书的申请者进行身份审核。

40. 密钥对

数字证书采用公共加密技术，它不像有的加密技术中采用相同的密钥加密、解密数据。它是采用一对匹配的密钥进行加密、解密，每把密钥执行一种对数据的单向处理，每把的功能恰恰与另一把相反，一把用于加密时，则另一把就用于解密。

公开密钥是由其主人加以公开的，而私有密钥必须保密存放。为发送一份保

密报文，发送者必须使用接收者的公开密钥对数据进行加密，一旦加密，只有接收方用其私有密钥才能加以解密。相反地，订户也能用自己私有密钥对数据加以处理。换句话说，密钥对的工作是可以任选方向的。这提供了"数字签名"的基础，如果要一个订户用自己的私有密钥对数据进行了处理，别人可以用他提供的公开密钥对数据加以处理。由于仅仅拥有者本人知道私有密钥，这种被处理过的报文就形成了一种电子签名--一种别人无法产生的文件。

数字证书中包含了公开密钥信息，从而确认了拥有密钥对的订户的身份。

41. 分组密码

分组密码是对固定长度的一组明文进行加密的算法，目前流行的分组密码算法有 DES、IDEA 算法。

42. 数字信封

结合了对称加密算法和非对称加密算法的优点的加密技术（对称加密算法的速度快，适合大数据量，但接收方同发送方的密钥协商困难；非对称加密算法运算量大，运算速度慢，不适合大量数据的加密，但公钥加密的数据只有对应的私钥解开，适合向确定的对象发送小批量数据）。

第2章　信息发布与信息管理

2.1 证书库

证书库用来存放经 CA 签发的证书和证书撤销列表(CRL)，为订户和网络应用提供证书及验证证书状态。可从此处获得其他订户的证书和公钥。

2.2 认证信息的发布

本 CPS 版权由广东省电子商务认证有限公司拥有，并负责解释，CPS 一经广东省电子商务认证有限公司在网站 http://www.cnca.net 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。本规范的发布及更改一律须经广东省电子商务认

证有限公司核准和发布。有需要人士可访问广东省电子商务认证有限公司网站 http://www.cnca.net 查看，对具体个人不另行通知。

2.3 证书和 CRL 发布

数字证书在签发成功后，广东省电子商务认证有限公司将该证书副本发布到证书存储区。广东省电子商务认证有限公司定期公布在证书有效期内被撤销的数字证书。在广东省电子商务认证有限公司的目录服务中可查询获得证书有关信息。

NETCA 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。

2.4 发布时间或频率

NETCA 在目录服务器上每工作日更新目录，每工作日发布最新 CRL。订户可在广东省电子商务认证有限公司的目录服务器上查询、下载数字证书和 CRL。

2.5 对证书信息的访问控制

NETCA 在其网站上发布与其相关的公众信息、处理旧信息。通过设置访问控制和安全审计措施，确保只有授权的 NETCA 工作人员才能编写、修改和删除 NETCA 在线发布的信息资料。同时 NETCA 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 NETCA 权限控制的信息资料。

第3章 身份标识与鉴别

身份标识与鉴别是指在颁发证书之前对最终证书申请者的身份和（或）其他属性进行鉴别的过程。本章亦描述对我公司下属之 RA 的身份鉴别过程和接受准则，还描述如何鉴别密钥更新请求者和撤销请求者及命名规则（包括在某些名称中对商标权的承认问题）。

3.1 命名

每张数字证书的主体中都包含一个主体名称（COMMON NAME），目的是标识证

书持有者的身份。

不同证书类型的主体名称命名规则不相同，但是所有证书的主体名称都必须经过审核。

3.1.1 各类数字证书的主体名称命名方式

各类数字证书的主体名称命名方式如下：

编号	证书类型	命名方式
1	个人证书	个人姓名（与身份证上标明的一致）
2	机构证书	机构名称（与营业执照等有效证件上标明的一致）
3	设备证书	域名或者 IP 地址，与盖章申请表上标明的一致

3.1.2 命名方式说明条款

(1) 主体名称必须能明确标识订户身份；

(2) 数字证书主体名称不能使用匿名或假名；

(3) 数字证书主体名称不能唯一的标识客户；

(4) 结合数字证书主体名称、电子邮箱、地址等信息，唯一标识客户；

3.2 身份的初始验证

个人证书订户按个人身份审核标准执行；机构证书、设备证书只提供给机构或部门性质的订户，对其证书订户按机构审核标准执行。

3.2.1 审核机构身份

1、 机构订户填写书面申请表（一式三份），经过机构授权代表的签署及机构盖章后，携带以下资料到 NETCA 或 NETCA 的 RA 进行身份审核及交费手续（以下证件的复印件和申请表需要机构盖章证明）：

i. 申请机构的组织机构代码证的复印件

ii. 申请机构的营业执照副本及复印件，如果没有营业执照，则提供书面申请表上可选的其他有效证件的副本及复印件；部分有效证件如下：

1) 营业执照
2) 企业法人营业执照
3) 事业机构登记证
4) 事业机构法人登记证
5) 税务登记证
6) 社会团体登记证
7) 社会团体法人登记证
8) 人民团体登记证
9) 人民团体法人登记证
10) 政府批文
11) 其他有效证件

iii. 经办人身份证原件与复印件

iv. 书面申请表

2、 NETCA 或 NETCA 的 RA 的业务受理人员认真、负责地核对申请资料的原件与复印件，根据审批人员的管理规定审核申请者的资料，并进行批准或拒绝的操作。

3、 NETCA 或 NETCA 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、实地考察或其它验证方式鉴定订户身份，申请机构有配合业务受理员的调查工作的义务。

3.2.2 审核个人身份

1、 NETCA 的个人证书签发给合法的个人申请者，NETCA 需要审核个人申请者的身份。个人申请者应填写书面申请表（一式三份），个人签字后，携带以下资料到 NETCA 或 NETCA 的 RA 进行身份审核及交费手续：

i. 个人身份证原件与复印件（或者是户口簿或护照）

ii.个人签字后的书面申请表（一式三份）

2、 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 NETCA 的审核，审核机构中的个人可以申请个人证书，其申请表必须由所属机构盖章。

3、 NETCA 或 NETCA 的 RA 的审批人员认真、负责地核对申请资料的原件与复印件，根据操作人员的管理规定审核申请者的资料，并进行批准或拒绝的操作。

3.2.3 审核认证体系成员身份

1、 NETCA 的 RA 工作人员必须是 NETCA 所属 RA 受理机构的正式职员。

2、 各级 RA 工作人员的身份除了必须符合个人证书申请者的条件外，还必须符合认证业务管理办法中的有关规定。

3、 RA 所属企业必须为独立的法人机构，其身份审核依据 3.2.1 的审核流程进行，并由 NETCA 进行实地的考察后可确认其身份。

4、 RA 的资格由 NETCA 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 NETCA 相关认证业务管理办法进行管理。

3.2.4 CA 相互认证的标准

NETCA 通过可能存在的国家根 CA、国家桥 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 NETCA 进行了 CA 的相互认证，须在 NETCA CPS 中列明。

3.3 数字证书（密钥）更新请求中的身份标识与鉴别

数字证书订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。

3.3.1 不同类型申请者的证书更新申请审核办法有所不同：

编号	申请者类型	审核要求
1	个人	向 NETCA 或其下属 RA 提交书面申请表及个人身份证的复印件，当面审核身份证原件；对从属于单位的个人证书，审核单位授权更新申请情况（盖章确认）。
2	机构	向 NETCA 或其下属 RA 提交书面申请表及申请机构的有效证件副本的复印件（例如营业制照副本）、经办人的身份证复印件，当面审核经办人的身份证及机构有效证件副本的原件。

3.4 证书撤销

数字证书订户申请撤销数字证书时，需要经过身份审核，才能够完成撤销的

过程。

3.4.1 不同类型申请者的证书撤销申请审核办法有所不同：

编号	申请者类型	审核要求
1	个人	向 NETCA 或其下属 RA 提交书面申请表及个人身份证的复印件，当面审核身份证原件。对从属于单位的个人证书，审核单位授权更新申请情况（盖章确认）。
2	机构	向 NETCA 或其下属 RA 提交书面申请表及申请机构的有效证件副本的复印件（例如营业执照副本）、经办人的身份证复印件，当面审核经办人的身份证及机构有效证件副本的原件。

第4章　证书生命周期操作规范

证书的生命周期是指数字证书的发放、证书的更新、撤销、中止或是对到期的证书进行撤销等操作。相关的具体操作规范，包括：证书申请、证书申请处理、证书签发、证书接受、密钥对和证书的使用、证书更新、证书密钥更新、证书变更、证书撤销和挂起、证书状态服务、订购结束及申请加密密钥和恢复等方面的操作规范。

4.1 证书申请

NETCA 建立 RA 受理实体的证书申请。实体为申请证书而提交的信息必须真实，否则后果由申请实体承担。NETCA 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。

NETCA 数字证书申请流程为：

1、 证书申请人在网上下载、填写书面申请表格。

2、 所有证书申请订户，需携带一式三份的书面证书申请表格及相关身份证明资料，到 NETCA 或其 RA 进行注册、身份审核和交费，具体身份审核所需资料依据 3.2 身份的初始验证。

4.2 证书申请处理

一般情况下，NETCA 处理订户的申请时间不超出五个工作日。根据数字证书申请方式，RA 审批的过程为：

1、 NETCA 或其 RA 对订户提交的身份证明资料和书面申请表格进行初次审核。
2、 审核通过，业务受理员在申请表中签名确认，并将申请表中的一份返还订户。审核不通过，拒绝订户申请。
3、 收费，并继续申请处理流程。
4、 业务受理员登录系统并根据订户提交的申请表格及交费情况，录入订户资料。
5、 业务受理员核对录入信息及纸面信息，进行系统身份审核。

4.3 证书签发

1、 对于审批通过的订户，RA 通过安全通道，将订户信息、RA 签名信息发送到 NETCA。
2、 NETCA 认证系统在验证 RA 签名并确认 RA 权限后，自动签发数字证书。
3、 在 CA 签发之前，CA 有权对订户进行二次审核，有权对认为身份审核不能通过的订户进行拒绝签发的操作。
4、 对于签发成功的订户，业务受理员进行制证操作，安装证书。

4.4 证书接受

4.4.1 证书的发布

证书签发后，NETCA 将证书发布到 LDAP 证书库。

4.4.2 申请者接受证书

1、 订户提交请求 5 个工作日后，凭申请时返还的证书申请表及经办人身份证到 RA 领取电子密钥，接受证书。
2、 经办人在证书领取记录上签名后，视为订户已接受数字证书。
3、 订户接受了证书后，必须妥善保存好证书对应的私钥。

4.5 密钥对和证书的使用

4.5.1 订户密钥对和证书的使用：

NETCA 为订户颁发双密钥体系证书，每订户的数字证书分签名证书及加密证书，签名证书密钥用法为：Digital Signature, Non-Repudiation；加密证书密钥用法为：Key Encipherment, Data Encipherment。订户结合签名证书及加密证书的功能，可实现以下功能：

编号	证书类型	订户私钥和证书的使用
1	个人证书	1）订户使用此证书来向对方表明个人的身份，同时应用系统也可以通过证书获得订户的其他信息。 2）主要用于：文档签名、发送安全电子邮件、个人网上购物、网上炒股等
2	机构证书	1）颁发给独立的机构、组织，在互联网上证明该机构、组织的身份。 2）主要用于：文档签名、发送安全电子邮件、网上工商事务、网上招标投标、网上签约、安全网上公文传送、网上缴费、网上缴税、网上购物和网上报关等。
3	设备证书	1）主要颁发给 Web 站点或其他需要安全鉴别的服务器，证明服务器的身份信息。 2）主要用于：实现安全站点、配合个人证书、机构证书、机构员工证书等客户端的证书实现安全购物站点、安全工商业务综合服务平台、安全公文报送系统等

4.5.2 证书及密钥的使用说明

数字证书的订户必须确保自己的私钥不被他人窃取。如果订户无法确定其私钥为安全的，请及时向 NETCA 申请撤销私钥对应的数字证书，以免因此造成损失。而数字证书可通过签名电子邮件、http://www.cnca.net 上发布等方式向他人公布。

4.5.3 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，通过公钥验证对方电子签名的真实性，实现通信的不可抵赖性，并实现通信双方数据传输的保密性和完整性。

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

4.6 证书更新

证书更新是在不改变证书中订户的公钥或其他任何订户信息的情况下，为订户签发一张新有效期的数字证书。

4.6.1 证书更新的条件

1、 证书已到期，但策略允许继续使用相同的用户信息或其它原因。

2、 证书的更新由订户自行提出。

4.6.2 证书更新的流程

1、 订户在通过填写书面更新申请表格并交费。

2、 订户提交相应更新申请资料到 RA，其中身份审核资料参考 3.2。

3、 审核通过，RA 为订户提交更新申请请求。

4.6.3 证书更新的发布和订户接受

1、 CA 签发证书。

2、 业务受理员进行证书下载。

3、 提交更新请求的 5 个工作日后，经办人到 RA 填写领取记录，领取书证书。

4、 NETCA 以 LDAP 方式发布已更新的证书。

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。

4.7.1 证书密钥更新的条件

订户自己申请、因私钥泄漏而撤销证书之后、证书到期且密钥也到期或其它原因。

4.7.2 证书密钥更新流程

1、 订户在通过填写书面更新申请表格并交费。

2、 RA 为订户提交密钥更新请求，获得业务受理号。

4.7.3 证书密钥更新的发布和订户接受

1、 NETCA 在获得订户更新后证书的业务受理号后，在 RA 端为订户进行交费审批。

2、 CA 签发证书。

3、 业务受理员进行证书下载。

4、 订户到 RA 领取证书。

4.8 证书的撤销

以下是证书撤销的原因说明：

1) 订户没有指明

2) 密钥泄漏

3) 从属关系改变

4) 证书更新/取代

5) 操作终止

6) 其它情况。这些情况可以是因法律或政策等要求 NETCA 进行的临时或永久性的证书撤销措施。

4.8.1 证书的撤销流程

1) 订户报失

i. 订户确定要报失其证书的情况下，须携带原证书业务受理号及相应身份证书资料，到 NETCA 或其 RA 填写数字证书报失申请表格。

ii. 业务受理员确认其订户身份。

2) RA 撤销证书

i. RA 工作人员进入 RA 审批系统，输入申请报失证书的业务受理号。

ii.RA 工作人员及订户确认该报失证书。

iii. RA 工作人员完成相关证书撤销操作

3) CA 撤销证书

i. CA 管理员每个工作日签发一次 CRL。

4.8.2 撤销的发布

1) 发布周期：1 个工作日

2) 最大期限：7 天

当订户需要使用证书或验证对方的数字证书是否有效时，请登录 http://www.cnca.net 上下载最新的CRL。

4.9 证书状态服务

NETCA提供证书状态查询服务，包括定期的CRL发布，提供在线的CRL分发点；提供OCSP服务，客户可通过NETCA的OCSP客户端进行在线的证书状态的查询。

对非在线订户，可直接在NETCA的网站上下载CRL文件，通过此文件可离线查询证书状态。

4.10订购结束

证书到期后，若订户不进行证书更新，则证书自动到期失效，订购结束，订户停止使用认证服务；与未到期的其它撤销订户对比，其证书不会进入CRL。

4.11加密密钥托管和恢复

NETCA证书订户的加密私钥对由广东省电子商务密钥管理中心产生。

NETCA订户必须声明委托NETCA向广东省电子商务密钥管理中心申请加密密钥对，并申请该密钥对的密钥托管服务。

证书订户的密钥的业务管理参考其所绑定的数字证书的业务管理办法，并遵循NETCA电子认证服务协议相关条款。

第5章　认证机构设施、管理和操作控制

本章描述非技术安全控制（即物理、过程和人员控制），NETCA使用这些控制手段来安全地实现密钥生成、主体鉴别、证书签发、证书撤销、审计和归档等功能。

5.1 物理控制

5.1.1 机房安全

NETCA的机房位于广州市，严格按照《中华人民共和国国家标准 GB 9361-88》规定，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；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。

NETCA的主机房有七道物理保护层，用以监控和管理NETCA机房的物理通道。除主机房外，同时具有数据备份机房，切实保证电子认证系统实时服务的连续性和可靠性。所有机房的建设和管理将严格按照国家标准及NETCA的规定要求执行。

NETCA机房属高级别安全机房，核心数据处理在屏蔽机房内进行。全机房采用高安全性的监控技术，包括24小时7天自动监控的摄像、指纹、可控权限和时间的门禁系统等监控技术及人工监控管理，确保机房的安全。

机房内部一律禁止参观。只有经NETCA授权的人员才可以在NETCA有相应权限的工作人员陪同下，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所有操作。

在NETCA体系的各实体中，只有具备相应权限的工作人员，才可凭有效的电子密钥进入相应授权区域进行许可的操作，所有操作皆会被记录。NETCA的角色权限管理员负责设置和检查各RA工作人员的权限。各实体管理员的权限和相应的责任在其与NETCA签订的协议中有详细严格的规定。

5.1.2 电源和空调

NETCA系统由市电及后备发电机双电源供电，以备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)，避免电源波动。

NETCA系统的空调系统使用中央空调和冷却设备，同时备有独立的机房空调，严格遵守机房控温要求。

NETCA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，确保其符合标准。

5.1.3 防水

NETCA机房采用符合国家标准的防水材料建造，内设抽湿系统，同时制定相应的管理条例，并与房产所有者协调，确保系统能防止水侵蚀。

5.1.4 防火

NETCA装有自动感应的气体灭火、报警装置，同时与专业消防部门协调，制定相应的管理条例和应急消防灭火响应措施，确保系统避免火灾的威胁。

5.1.5 介质存储安全

NETCA与介质生产厂商协商，制定相应的技术标准和管理条例，防止诸如温度、湿度和磁力等环境变化以及人为可能造成的危害和破坏，确保介质存储安全。

5.1.6 系统热备份

NETCA提供系统关键设备的热备份，预防主系统因不可预计因素所导致的异常情况，维持系统正常运行。当主系统工作异常时，将立即自动切换至备份系统，确保系统能正常工作，维持对外服务。

5.1.7 异地备份

NETCA提供数据的异地备份，该操作严格遵循NETCA备份标准和操作程序，确保可以在灾难恢复中能维持数据可用性和完整性。

5.2 流程安全控制

5.2.1 权限控制

NETCA系统的权限为内置。各管理员、操作员需凭其授权的权限进行相应的管理、操作。各种类型的管理员、操作员的权限是独立的。

5.2.2 规范性流程、规章制度

NETCA对数字证书的生产、电子认证服务系统运维工作制定一系列流程、规章制度（CP），日常工作皆严格遵循该流程、规章制度。同时设立安全管理小组，授权安全审计人员进行定期审计。

5.2.3 秘密分割

NETCA采用秘密分割技术进行管理，并将分割部分分派给多个授权的密码持有者，以增强其私钥的可信度并提供密钥的可恢复性，确保安全。

5.3 人事安全控制

5.3.1 人员资格要求

NETCA在录用人员前，如该岗位需要进行可信人员背景调查的，必须按公司《可信人员背景调查制度》和《可信人员职位划分原则与鉴别规范》的要求，进行严格的与录用岗位对应调查级别的可信人员背景调查，符合要求方予试用。对新入职的员工必须经过三个月的试用期，试用通过后予以正式委任。对不符合岗位可信度要求的人员安排调职或解除劳动关系。

NETCA与有关政府部门和调查机构合作，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。

5.3.2 保密制度

员工自入职之日起必须与NETCA签订严格的保密协议，离职时与NETCA签订离职声明，对企业重要的技术和商业秘密承担为期5年的保密义务。

5.3.3 培训与再培训

公司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。NETCA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。

5.3.3.1培训

NETCA 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》、《电子认证服务管理办法》、《电子认证服务密码管理办法》等相关法律法规的培训；NETCA 的 CPS；NETCA 的安全原则和机制；NETCA 的系统运行、维护、安全；NETCA 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。

5.3.3.2再培训

NETCA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NETCA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。

5.3.4 对未授权操作的处理

NETCA员工所有涉及到业务操作安全的操作均有记录。记录由NETCA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，NETCA将立即中止该员工进入NETCA证书认证体系。当事人的证书和操作权限即时冻结或撤销，所做的未授权操作将立即被撤销失效。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 审计记录的保存

NETCA系统的审计记录分在线保存和离线保存，其中在线保存是把审计记录放在数据库中保存；离线保存则是把数据库中某段时间的审计记录以文件转储的方式分开保存。审计结果文档由CA安全管理小组进行安全控制。

5.4.2 审计记录的保存期限

NETCA系统的审计记录在数据库保存的期限为5年；离线保存的保存期限为10年。

5.4.3 审计记录的备份

NETCA保证所有的审计记录都按照NETCA的备份和程序进行备份。

5.4.4 审计采集系统

NETCA 审计采集的系统包括：

1) 证书数据库系统
2) 证书管理系统
3) 证书签发系统
4) 证书申请系统
5) 证书审核系统
6) 证书发布系统
7) 证书查询系统
8) NETCA 网站
9) 网络安全防护系统
10) 其它 NETCA 认为有必要审计的系统

NETCA将全天候准备对上述系统进行检查和管理，在必要的时候应用相关工具来满足各项审计的要求。

5.4.5 审计结果的通知

NETCA系统审计的结果将尽快通知相关的负责人。如果审计过程中发现被攻击的行为，将可能递交司法部门处理，是否通知攻击者，将由NETCA决定。

5.5 存档

5.5.1 档案类型

NETCA系统档案的类型包括证书数据库文件、CA密钥、NETCA发行的证书、CRL、ARL、证书申请资料、审计记录等。

5.5.2 档案的保存

NETCA系统的档案采用分开异地保存，并由专人管理，未经管理人员授权，任何人不得接近保存的档案。

5.5.3 档案保存期限

NETCA系统的档案的保存期限为5年。

5.5.4 档案备份

NETCA系统的档案采用光盘、磁带、密码设备等介质的形式做成备份。

5.5.5 档案的时间戳

对于每一个NETCA系统的档案，都会加上一个数字时间戳，以标识是何时产生或者备份的档案。

5.5.6 档案采集系统

NETCA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

NETCA将每年对档案信息的完整性和安全性作验证。

5.6 灾难恢复

5.6.1 NETCA 遭攻击或发生事故时的灾难恢复

NETCA发生事故或受到攻击时，发生通信网络资源被毁坏、CA系统不能提供正常服务、软件系统被破坏、数据库被篡改等现象或者因不可抗力造成的灾难，NETCA将按照灾难恢复计划进行系统的灾难恢复。具体由NETCA的灾难恢复计划决定。

5.6.2 根私钥泄露的安全防范与补救措施

当NETCA的根私钥被泄漏时，NETCA将按NETCA的灾难恢复计划重新生成NETCA根私钥，并撤销NETCA体系下的所有证书，并要求重新签发。

5.7 CA 或 RA 业务终止

5.7.1 CA 业务终止

当NETCA打算终止业务情况下，NETCA应在终止业务前三个月给予RA和证书持有人书面通知，并按照相关法律规定的步骤操作，尽量减少对RA及证书持有人的影响。

NETCA按照相关法律规定来安排档案和证书的存档工作。

5.7.2 RA 业务终止

RA有权决定终止代理数字证书业务。RA应在终止业务前一个月给CA和其所办理证书的证书持有人书面通知，并按照相关法规的步骤操作，尽量减少对CA及证书持有人的影响。

RA有维护NETCA利益及信誉的义务。如果其行为导致订户投诉、被媒体曝光或被提起诉讼，有损NETCA公众形象的，NETCA有权视情节轻重暂停其代理业务或者取消其代理资格，由此造成的后果由RA自行承担。

RA应建立业务档案，对订户资料严格保密，并按照NETCA的要求，以可靠的方式及时将订户资料交给NETCA。RA的代理业务终止之日起10个工作日内，RA必须将所有订户资料无条件交给NETCA。

第6章 认证系统技术安全控制

6.1 密钥对的生成和安装

由于密钥对是安全机制的关键，所以必须在CPS中制定相应的规定，确保密钥对的产生、存储、分发、备份、更新、撤销、归档和恢复等具备保密性、完整性和不可否认性。

6.1.1 密钥对的生成

1) NETCA 及其 RA 皆持有签名密钥对，该密钥对是由国家密码管理局（以下简称国密局）许可使用的加密设备生成的，由各实体控制管理。

2) 订户可使用 NETCA 认可的或所提供的应用程序生产用于数字签名的密钥对和用于数据加密的密钥对。订户的密钥对的产生必须遵循《中华人民共和国电子签名法》、《电子认证服务管理办法》、《商用密码管理条例》、《电子认证服务密码管理办法》等相关法律、法规。

3) NETCA支持多种模式产生的密钥对,证书申请人可根据具体需求进行选择。证书申请人的签名证书密钥对可以由申请人自行产生，也可以由 RA 代为产生（此时密钥必须存储在国密局批准的不可导出的证书存储介质中，保证 RA 无法复制密钥对）;但证书申请人的加密证书的密钥对必须由密钥管理中心产生。任何模式操作都必须保证密钥对产生的安全性，不允许泄漏或复制申请人的私钥。NETCA 在技术、流程和管理上，确保了该安全保密性。

6.1.2 私钥的传递

1) NETCA 的 CA 根密钥是在系统创建时自生产的，该私钥只能保存在 NETCA 的 CA 系统中，禁止向外传递。

2) 各 RA 的密钥对由 NETCA 产生。RA 的私钥则由 NETCA 通过离线方式安全传送其私钥。

3) 如证书订户的密钥对是由 RA 代为产生的，则 RA 使用国密局批准的介质产生密钥对，安装用户证书后，封装好通过离线方式，发放给订户。

6.1.3 公钥的传递

公钥连同证书都是应该公布的，供有需要的人士下载使用。使用公钥对数据加以处理，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，再由相应的私钥进行解密，但仅限于该密钥用途为加密的时候。

6.1.4 CA 公钥的传递

NETCA的根CA的公钥包含在NETCA自签的根证书中。

6.1.5 密钥长度

NETCA各实体的密钥对至少为1024位的RSA密钥对。

6.1.6 公钥参数的产生

公钥参数由国家许可、NETCA认可的硬件产生。其中NETCA各实体的密钥皆由国密局批准的硬件加密设备产生，证书持有人的密钥可由国家许可、NETCA认可的硬件加密设备产生。

6.1.7 密钥用途

1) 在 NETCA 证书服务体系中的密钥用途和证书类型紧密相关，NETCA 的签名密钥用于签发下级 CA、RA 证书和证书撤销列表（CRL）；

2) RA 的签名密钥用于确认 RA 所做的审批证书等操作；

3) 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；

4) 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。

6.1.8 公钥的存档

公钥属于安全数据，NETCA体系中所有公钥都必须进行归档、存档。公钥的存档应严格按照数据存档步骤进行。

6.1.9 证书与密钥对的有效期限

CA根证书有效期为30年。RA和订户证书由于考虑到安全性，目前提供的证书有效期一般为一年或两年。

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

NETCA使用国家许可的产品，密码模块的标准符合国家规定的要求。

6.2.2 私钥的分割管理

NETCA采用多人控制策略激活、使用、停止NETCA的签名密钥。

6.2.3 私钥托管

密钥管理中心可以根据客户和法律的需要，对加密私钥进行托管。订户的签名私钥从不进行托管，以保证其不可否认性。NETCA可以协助客户进行加密密钥托管，但在技术上保证NETCA无法获取客户托管的私钥。

6.2.4 私钥备份

NETCA为确保签名的唯一性，不提供签名证书私钥备份服务。

用户可NETCA委托广东省电子商务密钥管理中心进行备份托管的私钥，并且要确保这些私钥的安全。

6.2.5 私钥存档

广东省电子商务密钥管理中心提供过期的托管私钥的存档服务。

6.2.6 私钥在密码模块中的导入/导出

在NETCA证书服务体系中，使用NETCA的软件可以把订户的加密密钥的私钥导入密码模块中；但订户的私钥无法从硬件密码模块中导出。

6.2.7 私钥在密码模块中的保存

NETCA的签名私钥必须保存在硬件密码模块中；订户的私钥保存在硬件密码模块中。

6.2.8 销毁私钥

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，订户必须删除电子密钥中的信息，以销毁密钥。NETCA的订户证书管理工具提供了电子密钥信息删除功能以便订户销毁私钥。

6.3 敏感数据的保护

6.3.1 敏感数据的产生

NETCA提供唯一的不可猜测的电子密钥，例如私钥密码。这些电子密钥由NETCA根据授权和操作的许可实施批准并且仅发放给授权订户。

6.3.2 敏感数据的保护

NETCA采取加解密机制等多种方式保护敏感数据，以避免未授权的使用。未授权订户企图使用敏感数据达到预定的数目时，敏感数据会自动锁定。

6.4 计算机设备安全控制

6.4.1 计算机设备安全性要求

NETCA的CA系统的数据文件和设备由系统管理员维护，未经系统管理员授权，其它人员不能操作和控制CA系统；而其它普通订户也没有系统帐号和密码。NETCA系统部署在多级不同厂家的防火墙之内，确保系统网络安全。NETCA系统密码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系统密码。

6.4.2 计算机设备的安全等级

NETCA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GB17859-1999）的第五级：访问验证保护级。NETCA使用的密码设备是通过国家密码管理局批准生产的密码设备。

6.5 系统升级与相关安全性控制

6.5.1 系统升级控制

NETCA的软件设计和开发过程遵循以下原则：

1）第三方的软件设计和开发

2）第三方的验证和审核

3）安全风险和可靠性设计

6.5.2 安全性管理控制

NETCA的配置以及任何修改和升级都会记录在案并进行控制，并且NETCA采取一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。

6.6 网络安全性控制

NETCA有防火墙以及其它访问控制机制保护，其配置只允许已授权的机器访问。只有经过授权的NETCA员工才能够进入NETCA证书服务器、NETCA应用服务器、NETCA证书目录服务器、NETCA操作中心等设备或系统。所有授权订户必须有合法的管理员密钥，并且需要通过密码验证。

第7章　认证机构审计和其他评估

7.1 审计者的身份与资质

认证机构审计者对NETCA进行审计。NETCA对授权的数字证书业务受理点流程和操作进行审计，频率由NETCA或法律制定的监管机构决定。

7.1.1 NETCA 的内部审计

内部审计组织为NETCA安全管理小组，主要审查实际运营操作是否与NETCA最新发布的CPS版本中规定的一致。

7.1.2 NETCA 的外部审计

对NETCA实施认证机构审计的审计者必须符合监管法律和行业准则规定的资质和经验要求，包括：

- 必须是经许可的、有营业执照的、具有计算机安全专业技术知识的审计人员或审计评估机构，且在业界享有良好的声誉。
- 了解计算机信息安全体系、通信网络安全要求、PKI 技术标准和操作。
- 具备检查系统运行的专业技术和工具。

7.2 审计者与 NETCA 的关系

认证机构审计者与NETCA应无任何业务、财务往来或其他足以影响评估客观性的利害关系。

7.3 评估审计的频率与条件

NETCA系统的评估审计周期为每周一次。如果出现特殊情况则另行作审计，引发评估审计事件的特殊情况包括疑似或真实的安全泄密、客户反馈异常情况等。

每年进行一次年审，全面评估安全事件，改进审计、评估的方法和策略。

7.4 评估审计记录的保存

NETCA系统的评估审计记录分为在线保存和离线保存，其中在线保存是把审计记录放在数据库中保存 ;离线保存则是把数据库中某段时间的审计记录以文件转储的方式分开保存。

7.4.1 评估审计记录的保存期限

NETCA系统的评估审计记录在数据库保存的期限为5年 ;离线保存的保存期限为10年。

7.4.2 审计记录的备份

NETCA保证所有的审计记录都按照NETCA的备份程序进行备份。

7.5 对问题与不足采取的措施

如果在评估和审计过程中发现执行规范有不足或存在问题，NETCA将根据审计报告实施补救措施，按照监管法律或普遍认可的国际贯例迅速解决问题。

当NETCA安全管理小组认为有必要暂时中断CA认证服务时，NETCA必须停止服务进行安全修补，直至NETCA安全管理小组认为系统达到运营要求。

当NETCA安全管理小组认为已有订户证书存在重大安全隐患，需要进行撤销、更新等操作时，NETCA必须遵照CA安全管理小组意见进行证书撤销、更新等操作。

7.6 审计结果

除非法律明确要求，NETCA一般不公开审计结果。

第8章 法律责任和业务服务条款

8.1 费用

NETCA数字证书的发放、验证和管理实行有偿服务，订户有义务按照规定向NETCA交纳相关服务费用，包括：证书颁发或更新费用、证书访问费用、撤销或状态信息访问费用、其他服务的费用（如对相关CP或CPS提供访问服务）；证书相关服务费用，遵照广东省物价局相关批文。

NETCA数字证书一旦发放，NETCA不办理退证、退款手续。

8.2 财务责任

8.2.1 保险范围

当因不遵守操作规程而造成的RA身份审核不当或因NETCA密钥泄露而造成的订户不应承受的损失，NETCA根据国家相关法规进行赔付。

8.3 商业信息的保密性

8.3.1 保密信息的范围

1. 订户的个人/机构信息和商业信息、NETCA 与业务代理机构间的商业信息等属机密信息，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，法律明确规定，一般不能在未经另一方许可的前提下擅自公开。
2. 与 NETCA 及其业务代理机构相关的审计报告、审计结果等信息是机密信息，除 NETCA 及其授权和信任的员工，不能泄露给其他任何人。这些信息除了审查目的或法律规定的目的，不能用于其他用途。
3. 除非法律明文规定，NETCA 没有义务公布或透露订户证书以外的信息。

8.3.2 不在保密范畴内的信息

1. 该信息在披露时已经是公有知识，或者向接受者披露前已为接受者所知晓。
2. 由 NETCA 网站或手册公布的信息：证书申请流程、证书使用指南等信息，此类信息仅供订户下载使用，不得转载或用于任何商业用途，NETCA 保留追究责任的权利。
3. 根据所有者的要求披露的信息：当机密信息的所有者出于某种原因，要求 NETCA 公开或披露他所拥有的机密信息，NETCA 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，NETCA 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。
4. 向法律执行机关披露的信息：当 NETCA 在国家的法律、规章或法规条款的要求下，或在法院的要求下必须披露本认证业务声明中具有机密性质的信息时，NETCA 可以按照法律、法规、或法规条令以及法院判决的要求，向执法部门公布相关的机密信息。这种披露不能视为违反了保密的要求和义务，NETCA 无须承担任何责任。

8.3.3 保护保密信息的责任

1. NETCA 执行严格的信息保密规章制度以确保只有经 NETCA 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。
2. 除非符合本认证业务声明的规定，否则 NETCA 或其业务代理机构皆不得揭露或出售商业信息，亦不得与他方分享上述资料。
3. NETCA 与其业务代理机构皆不得公布或被要求公布任何机密信息，除非在发表之前收到已授权且为合理的明确要求，而提出此要求的人(i)NETCA 对其负有对资料保密的责任；(ii)需要机密信息（如果不是同一人）或者是由于法院的命令。NETCA 或其业务代理机构在揭露此资料之前，可以要求此需要机密信息的人支付合理费用。
4. 除非法律明文规定，否则任何人不得擅自泄露任何的机密信息，一经发现必追究其责任。

8.4 个人信息的隐私性

8.4.1 隐私保护方案

1. NETCA 制定并落实严格的隐私保护规章制度，所有相关人员（包括 NETCA 及其业务代理机构的工作人员、订户）必须遵守该规章制度，NETCA 有权根据情况修改相关内容。
2. 由 NETCA 制定及实施的隐私保护规章制度符合国家保密机构的相关规定。

8.4.2 被视为隐私的信息

1. NETCA 及其 RA 证书资料库里面订户的个人/机构信息。
2. NETCA 证书申请者、订户和其他参与者的个人身份私有信息。

8.4.3 不是隐私的信息

1. 由 NETCA 网站或手册公布的信息：订户的数字证书、证书撤销情况等信息，此类信息仅供订户下载使用，不得转载或用于任何商业用途，NETCA 保留

追究责任的权利。

8.4.4 保护隐私信息的责任

1. NETCA 执行严格的信息保密规章制度以确保只有经 NETCA 授权的人员才能接近隐私信息。严格禁止未授权的访问、阅读、修改和删除等操作。
2. 除非符合本认证业务声明的规定，否则 NETCA 或其业务代理机构皆不得揭露或出售申请人姓名或其它识别资料，亦不得与他方分享上述资料。
3. NETCA 与其业务代理机构皆不得公布或被要求公布任何隐私信息，除非在发表之前收到已授权且为合理的明确要求。
4. 除非法律明文规定，否则任何人不得擅自泄露任何的隐私信息，一经发现必追究其责任。

8.4.5 使用隐私信息的通告或许可

1. NETCA 的证书资料库中应包含证书申请人的姓名、机构名称、证书有效期、证书状态等证书相关的资料。
2. 在发表之前收到已授权且为合理的明确要求，而提出此要求的人(i)NETCA 对其负有对资料保密的责任；(ii)需要隐私信息的人（如果不是同一人）或者是由于法院的命令。NETCA 或其业务代理机构在揭露此资料之前，可以要求此需要隐私信息的人支付合理费用。

8.4.6 依照司法或管理过程公开

向法律执行机关披露的信息：当NETCA在国家的法律、规章或法规条款的要求下，或在法院的要求下必须披露本认证业务声明中具有机密性质的信息时，NETCA可以按照法律、法规、或法规条令以及法院判决的要求，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，NETCA无须承担任何责任。

8.4.7 其他信息公开条件

根据所有者的要求披露的信息：当隐私信息的所有者出于某种原因，要求NETCA公开或披露他所拥有的隐私信息，NETCA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，NETCA不应承担任何与此相关的或由于公开隐私信息引起的所有损失、损坏的赔偿责任。

8.5 知识版权

1. NETCA 享有并保留对证书以及 NETCA 提供的全部软件的一切知识产权，包括所有权、名称权和利益分享权等。
2. “网证通”电子认证系统是由 NETCA 投资开发和运行的，因此 NETCA 拥有该软件系统的知识产权。
3. 所有由 NETCA 颁发的数字证书、提供的软件、相关的文件和使用手册均属于 NETCA 的知识产权范围。
4. 在没有 NETCA 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 NETCA 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。
5. 证书申请人（于接受申请时即为订户）声明并保证其交付（给 NETCA）使用的网域与辨识名称（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、商标名称、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。证书申请人（于接受申请时即为订户）应为 NETCA 辩护、赔偿并使其不受此类干扰或侵权而造成损失或损害赔偿。

8.6 陈述和担保

8.6.1 NETCA 的陈述和担保

8.6.1.1NETCA 享有的权利

1. 要求数字证书申请者提供真实资料的权利，有权按申请不同类型的数字证书，要求申请者提供不同的真实资料：对个人数字证书申请者，NETCA 要求其提供个人的姓名、个人身份证的原件以及复印件、身份证号、联系电话、住址、通信地址、邮政编码、电子邮箱等个人资料；对机构数字证书申请者，除对具体的经办人要求提供上述个人资料外，还要求提供申请机构资料——如机构名称、机构地址、机构组织机构代码、机构电子邮箱、电话、传真、机构有效证件的原件与复印件等资料；对服务器数字证书申请者，要求提供的服务器资料包括域名、IP 地址、WEB 服务器、操作系统、安装地点、所属机构名称、所属机构地址等资料，还同时要求提供申请机构和经办人的有关资料及其相关有效证件的原件和复印件。NETCA 或 NETCA 授权的受理审核机构在遵循合法程序的条件下有权对上述内容进行调查、审核。
2. 根据业务发展的需要，有权委托相关法人机构作为业务受理审批机构（即业务受理点）从事数字证书的受理、数字证书订户的身份审核和发放等。
3. 有权提供不同类型的数字证书，满足不同的数字证书订户的不同需要。
4. 收取费用的权利：NETCA 有权向证书申请者收取费用。
5. NETCA 在法律许可范围内可以有权对所有数字证书遭受破坏或盗用的情况协助调查，其调查包括但不限于面谈、记录与相关程序、相关设施的检查等。
6. NETCA 对于下列情况之一，将有权主动撤销所签发给订户的证书：
   1) 证书申请初始注册时，提供不真实材料；
   2) 违反国家法律或者其它规章制度，不应签发证书的；

3) 有盗用、冒用、伪造或者篡改他人证书的；

4) 不履行 NETCA 的内部规范，如《NETCA CPS》中的规定；

5) 与证书中的公钥相对应的私钥被泄密；

6) 证书中的相关信息有所变更；

7) 由于证书不再需要用于原来的用途而要求终止；

8) 证书的更新费用未收到；

9) 证书的实体消亡。

7．其他情况：

1) NETCA 有权确认：证书申请人确为证书申请书所说明的实体（依据证书类型描述的内容）；证书申请人合法地持有证书中所列的公开密钥所对应的私人密钥；除未经证实的订户资料外，证书中所记载的资料均准确无误，任何申请列有证书申请人公开密钥的证书的代理人是经过合法授权提出申请的。

2) 当使用或信赖证书的证书依赖方或 NETCA 的业务代理机构和雇员的违约行为或其他行为导致 NETCA 发生任何损失、损坏或债务责任和法律费用以及成本损耗，NETCA 有权要求赔偿。

8.6.1.2NETCA 义务

NETCA在从事电子认证活动时，与认证服务对象相比处于主动状态，因此，法律的作用就是要调整这种不平衡，以达到新的平衡。为此，法律规范的NETCA所履行的义务包括：

1．NETCA 最重要的任务就是制作、发放和管理认证证书。所以，它首要的义务就是保证认证证书的真实有效性，即所发放认证证书同某个确定身份的人是对应的，这就要求 NETCA 要对申请证书登记人的身份进行严格的审查和认证，保证发放的证书具有可靠的权威性和信任度，发布可靠及时的认证信息，这其中还包括了证实证书申请人所拥有的身份证、许可证或营业

执照等关系该人行为能力的文书或证件的效力。而为了更有效地确保认证证书的效力，NETCA 还享有撤消认证证书效力的权利。

2. NETCA 有保密的义务，除其他法律另有规定外，NETCA 不得对外披露以下信息：数字证书申请人向 NETCA 披露的身份信息及有关信息，数字证书上所列明的信息除外；在任何数字证书被撤销后的五年内，NETCA 应当保存该数字证书的相关信息。

3. NETCA 有告知的义务，NETCA 应该将使用电子签名及认证证书所应该了解的操作规程、需要的技术条件、以及其他一些确保电子签名及认证证书有效运作的必要注意事项告知密钥对的申请人及认证证书的申请人。NETCA 应当向社会公开披露以下内容并保证该内容的准确完整：

   1) 根证书；

   2) 数字证书上所列明的数字信息；

   3) 订户的公钥；

   4) 认证业务声明（CPS）；

   5) 撤销证书列表（CRL）；

   6) 其他任何影响数字证书安全性能或者 NETCA 服务能力的事实。

4. NETCA 应履行的义务还包括：在 NETCA 已同意批准签发的证书中，无不属实的陈述，证书申请人身份合法真实；经核准以后，接受订户的更新证书或撤销证书等的要求；如获悉任何对订户证书的有效性与可信度具重大影响的事实，应立即通知订户。

8.6.1.3NETCA 的主要法律责任

NETCA 的主要法律责任是负责查验证书申请人的身份，并对有关材料进行审查，为审查通过的订户制作、签发、管理电子签名认证证书，提供证书的目录信息查询服务和状态信息查询服务，更新证书和撤消证书等功能；管理黑名单库；保证自身和订户密钥的安全等等。

NETCA 在从事制作、签发、管理电子签名认证证书时，保证电子签名认证证书内容在有效期内完整、准确的业务活动中，承担着很大的法律责任风险。

关于 NETCA 怎样承担法律赔偿责任，只要符合以下情况，NETCA 应该适用无过错责任原则，若损害是由于当事人自己的行为所引起的，比如证书订户的个人密钥丢失没有及时通知 NETCA 引起的损失、订户提供的证书信息虚假问题出现的损失、订户非法使用证书产生的损失等等，则由各方当事人对其责任范围内发生的各项损害承担赔偿责任。或者，若 NETCA 已经尽到了合理谨慎注意的义务，对于判断合理谨慎注意的标准，法律作出了明确的规定，包括 NETCA 有否制定完善的认证业务操作规范和内部管理制度、有否使用合格的软硬件设备和从业人员、有否验证认证证书上记载信息的真实性等等，如果 NETCA 达到了这些要求，就可以认定为 NETCA 无过错而不需承担损害赔偿责任。但如果由于证书订户有证据证明 NETCA 有过错，或者因 NETCA 根私钥的失密等情况发生造成证书订户的损失，就应由 NETCA 承担损失赔偿责任。因此，按此方法可以较合理地调整 NETCA 所承担的责任。

8.6.2 NETCA 所属业务代理机构的陈述和担保

RA必须遵守由NETCA制定的所有登记程序和安全保障措施，NETCA有权根据情况修改有关内容。

8.6.3 订户的陈述和担保

8.6.3.1订户的权利

1. 获得有效合格的数字证书的权利：订户在提供了符合要求的信息资料并交纳证书服务费用后，有权利取得有效的、具有所需功能的数字证书。
2. 提出中止或撤销数字证书的权利：在上述的有关 NETCA 应中止或撤销数字证书的条件下，订户或其代理人有权提出中止或撤销证书的申请。

8.6.3.2订户的义务

在电子认证关系中，订户是NETCA的客户，是接受电子认证服务的一方。它除了应履行一般的支付服务费用义务外，还应履行一些与电子认证服务关系的特性相应的义务。这些义务主要包括诚实信用的义务、私钥保管的义务和通知的义务等等方面的内容。

1．诚实信用的义务（或真实陈述的义务）：

订户对证书内容真实性的保证：订户一旦接受了NETCA所颁发的证书，就要负担起保证证书中所含信息的真实性、准确性、完整性的义务。

订户对NETCA做出的所有重大陈述，包括订户已知的所有信息和在证书中的表述．无论是否经过NETCA的确认，都应当就其所知悉和所相信的范围保证最大程度的准确。对于违反这一基本义务当然应当负法律责任。这也是民法诚实信用原则的延伸。诚实信用义务最直接的表现为真实陈述义务：真实陈述NETCA颁发证书时要求其提供的事项，是订户在申请证书时所应履行的基本义务。因为就其身份、地址、营业范围、证书信赖等级的真实陈述，是证书可信赖性产生的前提，否则，将构成对证书体系信赖性的损害，并因此而承担一定的法律责任。

2．私密钥控制的义务：

订户对其私密钥应保持控制，确保私人密钥的安全，避免遭受破坏或盗用，并不得向未经授权的人泄露，并就私人密钥可能遗失、泄漏、修改或未经授权的使用等情况，采取合理的防范措施。否则，NETCA就是再认真审核、公正发布信息，都无法保证电子签名的安全性。

因此为了确保和强化订户的私人密钥的保护程度，NETCA常推荐一系列可靠的加密软件或硬件（如智能卡、USB电子密钥等）作为证书的存储介质，保证订户的私人密钥的安全。

当证书颁发并接收之后，订户就在真实陈述义务之外，之所以又增加了一项私密钥控制义务。它是订户所应负的针对不特定的任何人的义务。实际上，它是一种与NETCA的公正发布信息的义务相并列的社会责任。没有订户对其私密钥的独占性控制，NETCA就是再认真审核、公正发布信息，都无法保证电子签名证书

的安全性。控制私密钥，使其处于独占之安全状态，不仅是订户保护自身利益所必须的，同时，也是维护证书体系信誉的不可或缺的措施。订户若违反了该义务，将承担相应的法律责任。

3．通知的义务：

如果订户的私密钥出现问题，例如遗失、盗用、破坏或者泄密等，一旦订户私钥失密，就会出现他人冒订户之名进行交易的危险，因此，此时订户应当在察觉后的第一时间内通知所有所能预见到的受证书影响的人，包括NETCA；同时向NETCA申请中止或撤销该证书。

4．使用可信赖系统之义务：

订户在应用自己的密钥对时，也应使用可信赖系统。

5．交纳费用的义务：

订户应向 NETCA 交纳服务费用，主要在接受证书时交纳，在变更、中止或撤销证书时，订户也要向 NETCA 交纳当期费用。

8.6.3.3订户的主要法律责任

订户的主要法律责任如下：

1、订户在申请证书时，必须向 NETCA 提供真实、完整和准确的材料信息。

2、订户在证书申请表上填列的所有声明和信息必须在各方面都是完整、精确、真实和正确的，可供 NETCA 或其业务受理点查验。

3、订户必须严格遵守和服从所有 CPS 中规定的或者由 NETCA 推荐或使用的安全措施，以充分确保订户私钥的安全性。

4、订户需熟悉 NETCA 的 CPS 和与他们证书相关的证书政策，防止伪造、冒用、盗用他人电子签名等行为的发生。

8.6.3.4订户法律责任的承担

1、订户对所有信赖证书的人负有保证证书中信息的真实、准确、有效的法定义务，必须如实提交各种申请材料，如实填写申请表格，并必须对所提供资料的真实性、合法性负责，对因故意或过失提供虚假资料造成的任何后果承担法律责任；若订户违反了这些义务并由此造成了证书信赖者的损失，也应对证书信赖者负侵权之责。

2、订户应当妥善保管 NETCA 所签发的证书的私钥，不得泄漏或交付他人。如因故意、过失导致他人知道或遭盗用、冒用、伪造或者篡改数字证书或者与数字证书中的公钥相对应的私钥被泄密造成的任何后果，订户应当自行负责一切法律责任，NETCA 不负任何赔偿责任和法律责任。

3、订户如果需要申请改变 NETCA 签发证书与密码时，应按照规定申请流程办理。但在变更之前出现泄漏或遭他人盗用、冒用、伪造或者篡改时，仍应自行承担应负责任。

4、订户的私钥遭遗失、盗用、冒用、伪造或者篡改以及存储介质遭遗失，或者订户不希望继续使用证书时，应当立即通知 NETCA 废除证书。订户应当承担在证书废除之前所有使用其证书造成的责任问题。

5、订户违反证书使用相关规定，导致 NETCA 或者他人损失时，订户应自行承担赔偿责任。

6、证书一律不得转让、转借或转用。因转让、转借或转用而产生的一切损失均由订户负责。由于订户不象 NETCA 那样居于专业性服务机构的地位，因此对订户不应实行过错推定责任，而应采一般的过错责任原则，实行“ 谁主张、谁举证 ”的举证责任制度。

7、随技术的进步，NETCA 有权要求订户更换数字证书。订户在收到技术更新通知时，应在规定的期限内到 NETCA 更新数字证书，若逾期订户没有更新，所引起的后果由订户自行承担。

8、所有使用证书在网上进行的电子商务活动均视为订户所为，因此而产生的一切后果均由证书订户负责，证书订户必须遵守国家的相关法律法规规定。

9、若订户为个人，在个人死亡时，其法定责任人需要携带相关证明文件及原数字证书申请证明，向 NETCA 请求废除订户的数字证书。如数字证书申请证明遗失，凭法律效力证明废除订户数字证书。相关责任人应承担其数字证书在废除前产生的一切行为的责任承担事项。

10、若订户为单位，在单位解散时，法定清算人需要携带相关证明文件及原数字证书申请证明，向 NETCA 请求废除订户的数字证书。如数字证书申请证明遗失，凭法律效力文件证明废除订户数字证书。相关责任人应承担其数字证书在废除前产生的一切行为。

8.6.4 依赖方的陈述和担保

所有的证书依赖方在信赖任何证书的时候，须要遵守以下几点义务：

1．证书依赖方须熟悉电子认证业务声明以及和订户证书相关的证书政策，还须了解和遵守证书的使用目的。证书依赖方必须确保证书的确用于预定的目的。

2．证书依赖方在信赖订户的证书前，必须根据相应的最新的证书撤销列表（即黑名单 CRL）检查证书的状态，查明证书是否还有效。

3．当证书依赖方在网上进行电子商务时，有权审查自己或对方的证书是否在有效期内，是否已被列为“ 黑名单 ”，证书依赖方应该在做出决定是否相信某个证书之前，应该先查看“ 查询证书 ”以确定该证书是否有效的、未经撤销的或更新的证书，然后再用该证书来确认该电子签名是否在证书有效期内，是否与证书中所列的公开密钥相对应的私人密钥所产生的，加入电子签名的信息未被改动。必要时有权向 NETCA 联系和查询。

8.7 担保免责

8.7.1 法律免责事由

免责事由可分为不可抗力、免责条款和债权人的过错三种类型。

1． 不可抗力

不可抗力，是指不能预见、不能避免并不能克服的客观情况。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；也可以是社会现象、社会异常事件或者政府行为，如合同订立后政府颁发新的政策、法律和行政法规，致使合同无法履行，再如战争、罢工、骚乱等社会异常事件。不可抗力一般是法定的免责条款，例如我国《合同法》第 117 条规定：“因不可抗力不能履行合同的，根据不可抗力的影响，部分或者全部免除责任，但法律另有规定的除外。”

在电子认证活动中，NETCA 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。

第三人的行为即使对合同当事人是不可预见和不可避免的，也不属不可抗力，不能成为免责事由。例如我国《合同法》第 121 条规定：“当事人一方因第三人的原因造成违约的，应当向对方承担违约责任。当事人一方和第三人之间的纠纷，依照法律规定或者按照约定解决。”在电子认证活动中，若因第三方如电信、电力部门的行为而造成 NETCA 的操作失败或迟延的，NETCA 不能以不可抗力为由而免除违约责任。

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，详见 NETCA 与证书申请人签订的合同条款。

3．债权人过错

如果合同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，例如签署者有使用可信赖系统的义务，若因签署者的计算机系统达不到要求而使 NETCA 不能履行或不能完全履行颁发证书、管理证书及发布信息的义务，则 NETCA 可以免责。

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

在NETCA违反了前文8.6.1.3条例规定的职责，NETCA承担赔偿责任（法律免责除外）。赔偿限制如下：

1. NETCA 所有的赔偿义务不得高于这种证书适用的债务上限，这种上限可以由 NETCA 改动。
2. NETCA 只有在 NETCA 证书有效期限内承担这种损失或损害赔偿。

8.8.1 NETCA 之违约赔偿对象

NETCA 之违约赔偿对象首先包括申请证书的签署者，这是不用解释的。需要分析的是信赖方和被假冒者能否向 NETCA 提出违约赔偿之要求。

合同关系的相对性是指合同关系只能发生在合同当事人之间，只能由合同当事人一方（债权人）向另一方（债务人）提出请求或者提起诉讼。除法律另有规定或者当事人另有约定外，合同当事人以外的第三人不能依据合同向合同当事人提出请求或者提起诉讼，也不对合同当事人承担义务或者责任。根据合同关系的相对性，违约责任只能发生在合同当事人之间。此处应考虑的合同关系相对性的例外是为第三人利益的合同。显然电子认证合同并非是为了信赖方的利益而签订的，更非为了被假冒方的利益而签订的，因此，对电子认证服务合同仍应坚持合同关系相对性规则，信赖方及被假冒方不能成为 NETCA 的违约赔偿对象。

8.8.2 NETCA 之侵权赔偿对象

假设某人假冒他人名义向 NETCA 申请证书，NETCA 未尽到法定的义务而颁发了证书，假冒者利用该证书以被假冒者名义进行欺诈性的交易而致被假冒者财产损失，那么受害的被假冒者就会成为 NETCA 的侵权赔偿对象；在 NETCA 的作废证书表失灵的情况下，信赖方可能因此遭受财产损失而成为侵权赔偿对象；如果签署者因私密钥遗失而向 NETCA 申请撤销证书，而 NETCA 由于失误而发生了迟延并由此给签署者造成了现有财产的损失，那么签署者也会成为 NETCA 之侵权赔偿对象；因此，NETCA 之侵权赔偿对象包括三类人：签署者、信赖方及被假冒者。

具体参照标准是：对现有财产的损失，NETCA 都应给予赔偿；而对可得利益

的损失，只有 NETCA 在进行电子认证活动时能明确知道其所提供的数字证书、认证服务是给某人用于某具体交易的，才应对其错误认证所致的受害方（可以是签署者，也可以是信赖方）在该交易中所受的可得利益损失予以赔偿。反之，如果 NETCA 不清楚自己的认证服务将用于哪些具体交易，对该交易中的可得利益也就不能预见，因而也就不对可得利益负赔偿责任。如果 NETCA 不是故意地造成错误认证，那么 NETCA 所赔偿的现有财产的损失和可得利益的损失之和不应超过证书中列明的可靠性限制；如果 NETCA 属故意地造成错误认证，那么它所赔偿的现有财产的损失和可得利益的损失之和可以超过证书中列明的可靠性限制。

NETCA 明确规定，信赖方应认真检查作废证书表以确保证书有效并在证书的可信赖范围内行事，否则 NETCA 对信赖方的损失不负赔偿责任。此声明并不违反有关法律的强制性规定，其内容在实践中也应是每个信赖方在准备依据证书确认相对方身份时所应具备的基本常识，因此，上述 NETCA 的负责声明应是合法有效的。

8.9 赔偿

由于现有的各国电子认证立法在 CA 的赔偿责任之最高限额的问题上都没有明确规定，NETCA 认证业务规则中声明：如果 NETCA 不是故意地造成错误认证，则前述中的应予赔偿的现有财产的损失及可得利益的损失之和的数额不应超过证书中列明的所认购的相应金额的服务费用；反之，如果 NETCA 属故意造成错误认证则前述中的应予赔偿的现有财产的损失及可得利益的损失之和的数额可以超过证书中列明的所认购的相应金额的服务费用。

由于证书订户提供证据证明 NETCA 有过错，或者因 NETCA 根私钥的失密等情况发生造成证书订户的损失，因此 NETCA 声明为损失方应承担的法律赔偿责任之最高限额为各类型电子签名证书订购时相应的服务费用的 10 倍。

但以下情况例外：

1. 发现申请者资料虚假的情况下，业务代理机构有权拒绝提供服务，但无须退还已收取的各项费用。
2. 由于订户在申请证书过程中欺骗性的陈述其身份而导致 NETCA 为其签发

了不正确的证书，NETCA 将根据相关法规追诉订户责任。

3. 订户在 NETCA 允许的目的范围之外使用或证书使用不当，所发生的相关责任与 NETCA 无关。

8.10有效期和终止

NETCA的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。最新版本的CPS请访问NETCA网站www.cnca.net以获得，对具体个人不做另行通知。当新版本的CPS正式发布生效，则旧版本的CPS将自动终止。

8.11各参与方的单独通告与通信

为保证法律上有效性，信息的发送方必须将信息进行有效的数字签名；待接收方将有效签名的收件信息返回后，可认为发送方的操作完成，否则发送方有责任确认签名信息是否到达接收方。信息的接收方收到有效签名信息后，发出有效的签名收件信息，通信完成。

参与通信的各方需将签名信息进行保存，任何一方保存的完整的有效的签名信息均可作此电子事务发生的依据，另一方不能进行否认。

8.12修订

8.12.1 修订程序

NETCA有权在合适的时间修订、修改和改变本认证业务声明书中任何术语、条件和条款，而且无须预先通知任何一方。

8.12.2 通告机制和周期

1. NETCA 有权在 NETCA 的自主数据库中设置和公布修改结果，或以其他方式，如：修改 CPS 版本的形式或网站（http://www.cnca.net）上公布。
2. 所有的修正、修改和变化在公布后立刻生效。订户如不在修改结果后公布的限定天数内作废证书，就视为同意这种修正、修改和变化。所有以书面形式提供给订户的内容，按以下规则发送：
   1) 接受者是一个公司则向其登记的联系地址或办公室发送信息；

2） 接受者是个人则向其申请书上规定的地址发送；

3） 这些通知可能用快递或挂号信的方式发送。NETCA 有权选择通过电子邮件（e-mail）向订户发送通知，邮件地址在订户申请证书时已注明了。

3. 发送给 NETCA 的通知应以书面形式传递，所有有这些通知应采用快递或挂号信的方式发送。发送给 NETCA 的通知亦可以通过电子邮件（e-mail）传递，但这种通知只有在 NETCA 收到订户的 e-mail 通知后 24 小时内，收到订户书面材料，方为有效。

8.13争端解决程序

如果当事人之间无法很好的解决出现的问题和争端，应该提交仲裁机构，根据仲裁条例在时效内裁决。这些条例在本CPS中已经体现和规定了。仲裁的决定是终决性的，对每个当事人都有约束力。仲裁的议程应采用中文记录，而且仲裁决定应由有司法权的法院来判定，或者申请法院对其判决或执行命令时予以司法许可范围内的配合。

8.14管辖法律

本认证业务声明在各方面按照国家现行法律法律规定执行和解释。

8.15与适用法律的一致性

本认证业务声明在各方面服从国家法律的管制和解释。

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

8.16综合规定

8.16.1 整体协议条款

本文档及NETCA的相关业务管理办法、国家相关法规构成NETCA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NETCA下属RA因故撤销，则其管理的相应订户须接受NETCA的业务调配，通过另一RA获得相应服务；

若NETCA因政策性原因或其它不可抗力停止服务，NETCA之下属订户须按国家规定，接受相应接管CA的证书服务条款。

8.16.3 中止条款

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

8.16.4 执行条款

通信各参与方中，单方违背合同的弃权不能构成连续弃权或其它违背行为的预先弃权。

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。不可抗力一般是法定的免责条款，例如我国《合同法》第117条规定：“ 因不可抗力不能履行合同的，根据不可抗力的影响，部分或者全部免除责任，但法律另有规定的除外。 ”

在电子认证活动中，NETCA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。其他认证各方（如订户）就不得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。电子认证合同中的不可抗力条

款往往出现在与数字证书申请表一起提供给订户的服务协议中，也可被规定在NETCA的认证业务声明中。

第三人的行为即使对合同当事人是不可预见和不可避免的，也不属不可抗力，不能成为免责事由。例如我国《合同法》第121条规定：“ 当事人一方因第三人的原因造成违约的，应当向对方承担违约责任。当事人一方和第三人之间的纠纷，依照法律规定或者按照约定解决。 ”在电子认证活动中，若因第三方如电信部门的行为而造成NETCA的操作失败或迟延的，NETCA不能以不可抗力为由而免除违约责任。

为了表达明确，免责条件包括罢工或其他劳动纠纷、暴动、国内骚动、供应商故意或无意的行为、不可抗力、战争、火灾、爆炸、地震、洪水或其他大灾难，以及其他一些没有罗列的原因。

8.17其它规定

8.17.1 各种规范的冲突

若本认证业务声明的规定与其它规定、指导方针或协议相互抵触，订户必须接受本认证业务声明的约束，除非本认证业务声明的规定在为法律所禁的范围内，且除非该相冲突的协议（i）其签署日期在本认证业务声明首次公开发行之前，或（ii）该协议明确地优于本认证业务声明，因此必须由该协议规范所有当事人。

8.17.2 安全资料的财产权益

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 NETCA 的产权所有。本规范旨在保护订户的隐私，避免未经授权者公布其证书。
- **认证业务声明：**本认证业务声明的产权为 NETCA 所有。
- **辨识名称：**辨识名称为该定名实体（或其雇主或委托人）所有。
- **私人密钥：**不论该密钥是以何种实体媒介存放或保护，私人密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。
- **公开密钥：**不论该密钥以何种实体媒介存放或保护，公开密钥为订户（或

其雇主或委托人）所有。

- **NETCA 的公开密钥**：NETCA 作为自身的根节点的公开密钥，是 NETCA 的财产。这个公钥由 NETCA 授权分配，放在值得信任的硬体或软件中。

8.17.3 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NETCA或其业务受理点：(i) 毁谤、中伤、不雅、色情、侮辱、迷信、憎恶或种族歧视的言论，(ii) 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，或(iii) 其它违法言论。

（全文结束）