网证通
NET CA

网证通证书策略

V1.0版

生效日期：2024年7月16日

www.cnca.net

广东省电子商务认证有限公司

Guangdong Electronic Certification Authority

修 订 历 史

版本	修订日期	修订说明
V1.0	2024 年 7 月	首个版本

目　　录

第 1 章 概括性描述

1.1 概述

《网证通证书策略》（以下简称“NETCA CP”或“本 CP”）是广东省电子商务认证有限公司（以下简称“NETCA”[1]）制定的数字证书服务策略声明，适用于 NETCA 签发和管理的数字证书及相关参与主体。为批准、签发、管理、使用、更新、撤销证书和相关的可信服务，NETCA 制定业务、法律和技术上的要求和规范，这些要求和规范包含一整套在 NETCA 范围内一致适用的单一规则集，保护 NETCA 数字证书服务的安全性和完整性。本 CP 并不是 NETCA 和各参与方之间的法律性协议，NETCA 和各参与方之间的权利义务由他们之间签署的各类协议定义。

本 CP 满足互联网标准组织制定的 RFC3647《互联网 X.509 公钥基础设施-证书策略和证书业务声明框架》以及国内标准 GB/T26855-2011《信息安全技术公钥基础设施证书策略与认证业务声明框架》的框架和要求，并根据中国的法律法规和 NETCA 的运营要求进行适当的改变。

NETCA 作为一个证书服务机构（以下简称 CA），在本 CP 的约束下生成根证书和中级证书，签发订户证书。基于不同的类型和应用范围，作为证书持有人的订户可以使用证书进行网络站点安全保护、文档签名、身份认证、代码签名等不同的应用。依赖方依照本 CP 中关于依赖方的义务要求，决定是否信任证书。网证通电子认证业务规则（CPS）及网证通电子政务电子认证业务规则（NETCA E-GOV CPS）接受本 CP 的约束，详细阐述了 NETCA 作为电子认证服务机构如何提供证书以及相应的管理、操作和保障措施。所有 NETCA 证书的订户及依赖方必须参照本 CP 及相关 CPS 的规定，决定对证书的使用和信任。

1.2 文档名称与标识

1.2.1 名称

本文档的名称是《网证通证书策略》，简称为 NETCA CP。

1.2.2 标识

本 CP 中为每类证书的证书策略项分配一个唯一的对象标识符，本 CP 包含的证书策略具体如下:

L3：1.3.6.1.4.1.18760.1.10 或 1.3.6.1.4.1.18760.20.10.3

L2：1.3.6.1.4.1.18760.20.10.2

L1：1.3.6.1.4.1.18760.20.10.1

[1] NETCA 在表示机构时为“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。

粤港互认：2.16.156.339.1.1.1.2.1 (自然人) / 2.16.156.339.1.1.2.2.1 (法人)
统一印章策略：1.3.6.1.4.1.18760.20.10.50。

1.3 认证体系的成员

1.3.1 电子认证服务机构

NETCA 是根据《中华人民共和国电子签名法》、《中华人民共和国密码法》、《电子认证服务管理办法》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。NETCA 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 设立认证（安全）策略管理委员会，进行相关业务管理活动。NETCA 下设服务中心、服务分中心及业务受理点（RA），为公众提供相应的电子认证服务（受理、审核和颁发数字证书等）及服务咨询。

1.3.2 注册机构

NETCA 的注册机构（简称 RA），又称为业务受理点，是 NETCA 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、证书变更、证书补办、证书撤销、密钥恢复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。

NETCA 各 RA 点挂牌的名称为“NETCA 数字证书业务受理点”。

1.3.3 订户

订户也称为证书持有者，指拥有电子认证服务机构签发的有效证书的实体。包括从 NETCA 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 NETCA 订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

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 证书应用

网证通签发的数字证书适合应用在企业信息化、电子政务、电子商务及公共服务等领域，以实现身份认证、电子签名、数据加密等目的。

1.4.1 适用的证书应用

证书类型	订户性质	适用范围
个人证书	社会自然人	社会自然人在电子事务处理过程中，代表其身份，行使数字签名及数据加密等服务
机构证书	政府、企业、事业等机构政府、企业、事业等机构中个人	政府、企业、事业等机构或政府、企业、事业等机构中个人在电子事务处理过程中，代表其身份，行使数字签名及数据加密等服务
设备证书	个人、政府、企业、事业等机构所属的设备及其它资源	个人、政府、企业、事业等机构所属的在电子事务处理过程代表其设备及其它资源身份进行交互数据的加解密等服务
其它类型证书	满足相关应用的特殊需求而提供的其他应用类型	代码签名等

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

NETCA CP 由 NETCA 认证（安全）策略管理委员会负责起草、注册、维护和更新，版权由 NETCA 完全拥有。

1.5.2 联系信息

联系地址：广州市海珠区海洲路 38 号东升云鼎大厦 5 楼

邮编：510308

网站：www.cnca.net

电话：(+8620)-38861746

电子邮件：cps.netca.gd@chinaccs.cn

1.5.3 CP 批准流程

NETCA CP 起草后，交由 NETCA 法律顾问审核通过，认证（安全）策略管理委员会通过后形成决议，在 NETCA 网站（www.cnca.net[2]）发布后，该 CP 正式生效。

在 NETCA 证书相关政策和操作规范做出任何变动之前，NETCA 认证（安全）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，并根据决策结论按需要遵循上述流程更新并发布 NETCA CP。

1.5.4 CP 的发布

NETCA 将对 NETCA CP 进行严格的版本控制，由 NETCA 认证（安全）策略管理委员会指定专人负责版本控制及发布。

所有 CP 相关公告和通知需获得认证（安全）策略管理委员会批准，方能在 NETCA 网站 www.cnca.net 上公布。

根据《中华人民共和国电子签名法》及《电子认证服务管理办法》的规定，NETCA 在公布 CP 后向工业和信息化部备案。

1.6 定义和缩写

1. CA（Certification 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、撤销等一系列管理。

2. RA（Registration Authority）

注册机构的简称。RA 是 CA 认证体系的对外服务机构，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，以及证书更新和撤销工作。

3. KMC（Key Management Center）

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

4. NETCA

广东省电子商务认证有限公司的简称。

5. CNCA

广东省电子商务认证有限公司的另一个域名标识。

[2] 网证通的另一站点域名 www.netca.net 与 www.cnca.net 是等效的，同样可用。

6. 网证通

广东省电子商务认证有限公司的电子认证服务品牌名称。在指实体名称时即代表广东省电子商务认证有限公司。

7. 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签发及管理数字证书的规范，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。

8. CRL（Certificate Revocation List)

数字证书撤销列表的简称。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序列号，供数字证书订户、依赖方在验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、下次撤销列表的预定签发日期、被撤销的数字证书序号，并说明被撤销的时间与可能存在的理由。

9. 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。

10. 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。

11. 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。

12. 加密

对数据进行密码变换以产生密文的过程。

13. 加密证书

用于证明加密公钥的数字证书。

14. 签名证书

用于证明签名公钥的数字证书。

15. DTS (Digital Time Stamp)

数字时间戳的简称。用于向订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。

16. 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撤销列表（CRL）。

17. 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"1.3.6.1.4.1.18760"）。OID 标准的定义来自 ITU-T 推荐 X.680 (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它对象标识符。

18. 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。

19. 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，及/或解密通过相应公钥加密的电子记录或文件。

20. 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。

21. 密码模块

实现密码运算功能的、相对独立的软件、硬件、固件或其组合。

22. 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。

23. URL（Uniform Resource Locator）

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

24. 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 USB KEY。

25. X.509

X.509 是 ITU 制定的 X.500 系列的目录标准的其中一个。它为公钥证书定义了一个框架。

26. 鉴别

辨别认定证书申请者提交材料真伪的过程。

27. 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。

28. SM2 算法

中国国家密码管理局发布的椭圆曲线公钥密码算法。参见《GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法》。

29. SM3 算法

中国国家密码管理局发布的密码杂凑算法。参见《GB/T 32905-2016 信息安全技术 SM3 密码杂凑算法》。

30. PKCS#10

证书请求语法规范，由 RSA 安全公司制定，它定义了证书签名请求的结构。也见 RFC 2986。

第 2 章 信息发布与信息管理

2.1 信息库

NETCA 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。NETCA 信息库内容包括但不限于以下内容：证书、CRL，证书状态信息，CP、

CPS，以及其它由 NETCA 不定期发布的信息。NETCA 证书库为信息库的子集，用来存放经 NETCA 签发的证书和证书撤销列表（CRL），主要为订户和依赖方提供 NETCA 证书查询及验证证书状态服务的信息库。订户和依赖方可登录 NETCA 网站（www.cnca.net）查询证书信息或下载证书。

NETCA 信息库不会改变任何从发证机构发出的证书和任何证书挂起或撤销的通知，而是准确描述上述内容。

2.2 认证信息的发布

2.2.1 CP 的发布

NETCA CP 一经 NETCA 在网站 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。NETCA CP 的发布及更改遵循本文 1.5.3 和 1.5.4 的规定。有需要人士可访问 NETCA 网站 www.cnca.net 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，NETCA 默认将该证书副本发布到信息库。NETCA 定期发布 CRL 以公布在证书有效期内被撤销、挂起的数字证书。证书依赖方可在 NETCA 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 NETCA 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。

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。

NETCA 也会发布来自电子认证服务主管部门的相关信息，包括对 NETCA 本身的证书进行挂起、撤销或不获续期的通知和 NETCA 发出的证书的可靠性或服务能力造成重大及不利影响的事件。

NETCA 也可根据需要，将 CA 系统中的数字证书、CRL 同步到电子政务下信息系统中。

2.3 发布时间或频率

2.3.1 CP 的发布时间或频率

NETCA 将及时发布 CP 的最新版本，一旦对规则的修改、补充、调整等获得批准，NETCA 将在 www.cnca.net 上发布，并将最新的 CP 发布在 NETCA 信息库。

NETCA 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 CP 的改动，其发布时间和频率将由 NETCA 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 NETCA 没有发布新的 CP，或者没有任何形式的公告、通知等形式宣布对 CP 进行修改、补充、调整或者更新前，当前的 CP 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，NETCA 在 4 小时内将该证书副本发布到信息库。订户也可以在其它信息库中公布其获得的 NETCA 签发的证书。

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

2.3.3 CRL 的发布时间或频率

NETCA 会在每批次挂起或撤销证书后，签发最新 CRL 并发布到 NETCA 的 LDAP 服务器或指定的信息库位置。从证书被挂起或撤销，到反映该证书状态的最新 CRL 发布的最大延迟不超过 24 小时。并且不管如何，对于反映终端实体证书状态的 CRL 最长会在 24 小时内重新签发一次，对于反映 CA 机构证书状态的 CRL 最长会在一年内被重新签发一次。

通过 OCSP 协议，请求者可以实时查看和获得某一证书的状态，包括有效、基于各种原因被撤销、挂起的状态。在满足要求以后，NETCA 还可以提供跟进服务，当指定的证书生效、被撤销、挂起/取消挂起时，NETCA 将按照约定的方式通知请求该项服务请求者。

2.4 对信息的访问控制

NETCA 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 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。

对于 NETCA 发布的 CP、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。

第 3 章 身份标识与鉴别

3.1 命名

3.1.1 名称类型

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。

3.1.2 对名称意义化的要求

订户的甄别名（DN）必须具有一定的代表意义，可与证书持有者的特有属性相关联。

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

3.1.3 订户的匿名或伪名

在 NETCA 的证书服务体系中，原则上订户不宜使用匿名或伪名。

3.1.4 解释不同名称形式的规则

数字证书的命名遵循《GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式》、《GM/T 0015-2023 数字证书格式》的要求。

3.1.5 名称的唯一性

在 NETCA 的证书服务体系中，证书主体名称必须是唯一的。但对于同一订户可以用其主体名为其签发多张证书，其证书内容会有所不同。

3.1.6 商标的识别、鉴别和角色

NETCA 机构签发的证书不包含任何商标或者可能对其他机构构成侵权的信息。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

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

NETCA 机构要求证书申请人妥善保管自己的私钥，因此，证书申请人视作其私钥的唯一持有者。

3.2.2 机构的身份确认

NETCA 或 RA 机构应验证证书申请人提交的机构有效证件或证件的具体信息、机构授予授权代表的授权证明和授权代表的身份证明材料，核实机构是确实存在的、合法的实体及确认申请人的意愿。

1. 机构有效证件的类型如下：
   - 营业执照
   - 事业单位法人证书
   - 社会团体法人登记证

- 民办非企业单位登记证书
- 政府批文
- 其他有效证件

2. 经办人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
   - 其他有效身份证明资料

机构身份的鉴别流程应当明确记录在按照本 CP 制定的 CPS 中。

3.2.3 个人的身份确认

NETCA 或 RA 机构应验证证书申请人提交的个人有效证件或证件的具体信息，核实个人身份的真实性，及确认申请人的意愿。

1. 个人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
   - 其他有效身份证明资料

个人身份的鉴别流程应当明确记录在按照本 CP 制定的 CPS 中。

3.2.4 机构中个人的身份确认

NETCA 或 RA 机构应验证证书申请人提交的机构有效证件或证件的具体信息、机构授予授权代表的授权证明和授权代表的身份证明材料，核实机构是确实存在的、合法的实体及确认该机构知晓并授权证书申请。机构、授权代表及机构中个人有效身份证件，详见 3.2.2、3.2.3 章节。

机构中个人身份的鉴别流程应当明确记录在按照本 CP 制定的 CPS 中。

3.2.5 设备的认证

申请人申请设备证书，除依据申请人身份的不同类别，按本文 3.2.2、3.2.3、3.2.4 证明申请人的身份外，还须证明对相应设备的识别信息拥有权。

3.2.6 不予验证的订户信息

未在前面所列的，对于不影响订户身份追溯的信息，NETCA 一般不予验证。

3.2.7 审核认证体系成员身份确认

1、 RA

- RA 的身份审核依据本文 3.2.2 的要求进行。
- RA 的资格由 NETCA 审查批准，正式获得相应资格后，其运作遵循 NETCA 的相关规定。

2、 业务受理人员

- 业务受理人员的身份除了满足 3.2.3 的要求外，还必须符合 NETCA 的相关规定。

3.2.8 CA 相互认证的要求

NETCA 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。

NETCA 在进行相互认证时遵循相关法律法规的规定，如果相关法律法规未列明的要求则采取对等的方式，以不降低信任管理类别为标准。

3.3 证书（密钥）更新请求中的身份鉴别

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。

NETCA 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。

3.4 证书撤销请求中的身份鉴别

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。

NETCA 可以采用以下方式之一来对撤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撤销申请，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。

第 4 章 证书生命周期操作规范

4.1 证书申请

NETCA 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、机构或其它客观存在的实体，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。

申请人须清楚了解及同意订户协议的内容，特别是关于责任和担保的内容、并根据申请的证书类型提供真实、可靠、完整的身份资料，承担任何因提供虚假、伪造信息所产生的法律责任。

4.2 证书申请处理

4.2.1 身份审核

NETCA 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

NETCA 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 NETCA 提交证书签发请求。

任何不能提供足够的身份证明材料，或未能完全满足关于订户信息的标识和鉴别的规定，或被 NETCA 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，或申请者未能接受订户协议的内容和要求，特别是关于义务和担保的内容，或未满足 NETCA 其他申请要求条件的，NETCA 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，NETCA 处理证书申请的时间不超出五个工作日，处理电子政务申请的时间不超出两个工作日，或按双方约定的处理时限。

NETCA 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

NETCA 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。

NETCA 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。NETCA 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，NETCA 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 NETCA 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。

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 NETCA 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订户接受数字证书：

1. 经办人在证书领取记录上签字；
2. 订户获取数字证书；
3. 订户从网上下载该数字证书；
4. 与订户约定的其它方式。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户只有接受了数字证书后方能使用证书对应的私钥。订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。订户使用数字证书时必须遵守国家相关法律法规、NETCA CP、相关 CPS 和签署的协议。

1. 订户私钥的使用应符合证书中“密钥用法”（KeyUsage）的要求，未按规定用途使用造成的损失，由订户自行承担；
2. 订户私钥和证书的使用应符合订户协议的要求；
3. 订户在使用证书的公钥所对应的私钥进行电子签名时，即保证是以订户的名义进行电子签名，并且在生成电子签名时，应已确保该证书没有过期或被挂起、撤销（若证书已到期或被挂起、撤销，订户应停止使用私钥）；
4. 订户应保持对其私钥的控制，并采取合理的措施来防止私钥的遗失、泄露、被篡改或未经授权被使用；
5. 订户不允许将证书用于非法活动；
6. 订户无法确定其私钥为安全时，应及时向 NETCA 申请撤销私钥对应的数字证书，以免因此造成损失。

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 NETCA 签发；
2. 检查该证书在有效期内；
3. 查验该证书没有被撤销、挂起。

证书依赖方依据 NETCA 的相关保障措施，再结合自己的交易风险，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订户的行为，对于不符合证书或密钥用法的证书使用，依赖方可以拒绝接收。

当依赖方需要发送加密信息给接受方时，可以通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息进行加密。

4.6 证书更新

证书更新是在不改变证书中的公钥，或说证书中任何订户信息不变的情况下，为订户签发一张有效期更新后的数字证书。

4.6.1 证书更新的情形

1. 证书将要到期或 NETCA 其它策略要求原因，且密钥对处于安全状态并且策略允许继续使用；
2. 订户或其授权代表提出证书的更新申请；
3. NETCA 的策略要求或相关法律法规引致其它原因。

证书已撤销或已挂起不适合该情形。

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，只适合于证书未被撤销或未被挂起的情形。通过 NETCA 网站或 NETCA 证书更新软件提交更新申请，经过 NETCA 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 NETCA 签发新的证书。订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。即订户或其授权代表提交证书更新申请表和身份证明材料，到 NETCA 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、发布和订户接受

1. 证书更新的签发与本文 4.3 相同；
2. 证书更新的发布和订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

证书密钥更新是指订户生成一对新密钥并申请为新公钥签发新证书，即更新证书同时也会更新数字证书密钥。NETCA不接受订户提供的私钥，也不接受订户的密钥的更新请求。

4.7.1 证书密钥更新的情形

1. 订户或其授权代表提出证书密钥的更新申请；
2. NETCA 的策略要求或相关法律法规引致其它原因。

证书已撤销或已挂起不适合该情形。

4.7.2 证书密钥更新请求的处理

证书密钥更新请求的处理与本文 4.6.2 相同。

4.7.3 证书密钥更新的签发、发布和订户接受

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

4.8 证书变更

证书变更是指证书订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 证书变更的情形

订户因其信息发生变化由其或其授权代表提出证书的变更申请。

4.8.2 证书变更请求的处理

其处理方式同本文 4.2 的要求，同时撤销原证书（参见本文 4.10 ）。

4.8.3 证书变更的签发、发布和订户接受

1. 证书变更涉及的证书签发与本文 4.3 相同；
2. 证书变更后订户的新证书发布和订户的证书接受与本文 4.4.1、4.4.2 规定相同。
3. 证书变更后因撤销原证书引起的 CRL 签发与发布同本文 4.10.5 。
4. 如果证书变更仅涉及非证书记载内容的变化，则 NETCA 可以不重新签发新证书，NETCA 或其 RA 不予发布相关信息，除非与订户或依赖方另有约定。

4.9 证书补办

证书补办是指在证书有效期内，证书持有者出现证书载体丢失或证书载体损坏时进行证书补发的操作。

4.9.1 证书补办的情形

订户因证书载体丢失或损坏时由其或其授权代表提出证书的补办申请。

4.9.2 证书补办请求的处理

证书补办请求的处理与本文 4.8.2 相同。

4.9.3 证书补办的签发、发布和订户接受

证书补办的签发、发布和订户接受的处理与本文 4.8.3 相同。

4.10 证书的撤销和挂起

4.10.1 证书撤销的情形

1. 证书订户提供的信息不真实；
2. 证书订户没有或无法履行有关规定和义务；
3. NETCA、NETCA RA、订户所属组织机构或最终证书订户有理由相信或强烈怀疑一个证书订户的私钥安全已经受到损害；
4. 证书密钥泄漏或存储证书的密码设备或模块丢失；
5. 证书主体名称列明的从属关系改变；
6. 证书主体的变更；
7. 任何与提供证书服务相关的协议到期；
8. 订户或其授权代表提出证书撤销申请；
9. 订户违反 NETCA CPS 或签订的相关证书协议；
10. 其它情况。例如因法律或政策等要求 NETCA 进行临时或永久性的证书撤销措施。

证书的撤销既可以是订户提出申请，也可以是订户所属组织机构发起证书撤销申请，也可以是NETCA因为有合理理由相信其发出的订户证书已经不可靠或订户的变更事实或违反约定事实而强制撤销。

4.10.2 证书撤销的处理

在发生证书需撤销的情形时，订户或其授权代表应及时按本文 3.2 的要求提供身份证明材料，向NETCA或其RA提交申请。

NETCA或其RA按本文 3.2 的要求进行身份审核通过后，即时在系统中完成证书的撤销操作。

当NETCA或其RA强制撤销某一证书时，将在完成撤销操作后按其登记的联系方式通知订户，如订户登记的联系方式变更而未通知NETCA，或登记的联系方式联系不上订户的，责任将由订户承担。

4.10.3 撤销请求的宽限期

在发生需要撤销证书的情形时，订户应第一时间通知NETCA或其RA，如果订户未能在当天前往NETCA或其RA进行撤销登记，则需要通过电话请求挂起证书。

4.10.4 证书挂起的处理

订户在丢失电子密匙或其它密钥泄露的情况下而来不及向NETCA或其RA进行撤销时，可以先请求挂起证书。

所有证书挂起申请要求NETCA或其RA受理人员核对申请人（或来电者）的身份进行确认。在完成身份核对后，NETCA或其RA受理人员即时进行证书的挂起操作。

订户在申请办理证书挂起后，应在72小时内，按本文 3.2 的身份审核要求向NETCA或其RA完成证书的撤销申请或取消挂起的申请。若订户未在72小时内来NETCA办理撤销手续的，NETCA将取消该挂起。

4.10.5 证书撤销和挂起状态的发布

任何时候证书被撤销或挂起，NETCA在30分钟内将该信息发布到NETCA信息库，并重新签发CRL。包含该撤销或挂起证书状态的CRL最迟在24小时内可以通过证书列明的URL获取。

当撤销的证书过期或挂起的证书被取消挂起时，相关证书会从下次发布的CRL中被撤出。

4.10.6 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 NETCA 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 NETCA 提供的 OCSP 服务，依赖方可以采用 OCSP 协议获得 NETCA 签发的所依赖证书的状态。

4.11 证书状态服务

NETCA提供7*24小时的证书状态查询服务。

订户和依赖方可以从NETCA的网站或目录服务器下载CRL查询证书状态，或使用NETCA（或第三方）的OCSP客户端工具（或接口）进行在线的证书状态的查询。对非在线订户或依赖方，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。

NETCA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。NETCA可为某些应用场合提供定制的OCSP服务。

4.12 订购结束

以下两种情况，表明证书订购结束：

1. 证书在有效期内被撤销[3]；
2. 证书有效期满后，订户不再进行证书更新或证书密钥更新。

[3] 该情形指“4.10.1 证书撤销的情形”描述的内容。

4.13 密钥生成、备份和恢复

4.13.1 密钥的生成和备份

NETCA颁发的订户证书中，含有签名用途的密钥对由订户生成或由NETCA提供的密码设备或模块生成，NETCA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。密钥管理中心由密码主管部门管理。

4.13.2 密钥的恢复

这里的密钥恢复即指订户的加密密钥对恢复。订户在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：

1. 订户密钥恢复：按本文 3.2 的身份初始验证所述之身份证明材料向NETCA申请办理。

2. 问责取证密钥恢复：问责取证人员向认证机构提交申请，经审核后，恢复的密钥记录于特定载体中。

密钥恢复服务根据KMC主管部门规定进行。

4.13.3 密钥对的存储和恢复安全策略

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

对于每次密钥对的申请和恢复，KMC使用订户或NETCA提供的密码设备或模块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。

其他用途的订户私钥不适用于本条款。

第 5 章 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

NETCA机房的选址和建设按照国家标准的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。

NETCA的主机房根据业务功能划分为接入区、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，且至少每五年进行一次屏蔽室检测。机房的建设和管理将严格按照国家标准及NETCA的规定要求执行。

5.1.2 物理访问

进出物理安全层的行为都需要被记录、审计和控制，从而保证进出每一个物理安全层的人都是经过授权的。NETCA的CPS应该对物理访问控制进行详细的规定。

5.1.3 电源和空调

NETCA系统由市电及后备发电机两路不同电源供电，当单路电源发生故障时也能及时自动切换，提供紧急供电，维持系统正常运转；同时备有不间断电源（UPS），避免电压波动。

NETCA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。

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，确保其符合设备运行要求。

5.1.4 水患防治

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

5.1.5 火灾预防和保护

NETCA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NETCA制定了火灾事故专项应急预案，在NETCA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

NETCA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。NETCA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，NETCA在它们作废前或保存期满后进行销毁。NETCA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

NETCA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

NETCA在CA机房内部署了入侵侦测报警系统，并进行安全布防。安全区域的窗户附近安装有玻璃破碎报警器，发生非法入侵会自动报警，保护NETCA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NETCA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. 密钥管理员
8. 安全审计员
9. 业务办理服务人员
10. 系统维护人员
11. 数据库维护人员
12. 物理环境维护人员
13. 网络维护人员

5.2.2 角色要求的人数

NETCA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；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卡（或智能门禁卡+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（或电子密匙）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

NETCA及NETCA的注册机构建立并执行严格的控制流程，根据工作要求和工作安排采取职责分离措施，建立互相牵制、互相监督的安全机制，确保由多名可信人员共同完成敏感操作。NETCA进行职责分离的角色，包括但不限于下列人员：

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

NETCA要求充当可信角色的人员至少必须具备忠诚、可信赖及工作的热诚度、无影响NETCA运行的其它兼职工作、无同行业重大错误记录、无违法记录等。

NETCA在录用担任可信角色的员工之前，除需满足一般的技能和经验要求外，对录用岗位的可信员工进行对应调查级别的背景调查，符合要求方予录用。可信员工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、征信记录等。

5.3.2 背景调查程序

拟录用担任信任角色的员工需同意NETCA作背景调查。NETCA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，始可录用。

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。

NETCA不定期进行可信员工背景调查，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

NETCA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。

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；《中华人民共和国电子签名法》、《中华人民共和国密码

法》、《电子认证服务管理办法》及《电子认证服务密码管理办法》、《电子政务电子认证管理办法》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。

5.3.4 再培训要求

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。

5.3.5 对未授权操作的处理

NETCA对所有涉及到业务操作安全的操作均有记录。记录由NETCA安全审计员审查。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证书认证体系各系统。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、解雇等，涉及犯罪的将送司法机关处理。

5.3.6 人员异动管理

NETCA会维护所有职员及可信雇员清单，对于离职员工，NETCA将立即删除其接触公司资料的权限。

5.4 审计日志程序

5.4.1 记录事件的类型

NETCA日志记录的事件包括但不限于以下内容：

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

每个事件的记录至少包括以下信息：

- 发生的日期和事件
- 事件的内容
- 事件相关的实体
- 事件的标识

5.4.2 日志的处理周期

NETCA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。

5.4.4 审计日志的保护

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

5.4.5 审计日志的备份

NETCA每月对纸质日志实施归档；对于审计日志，NETCA每天对审计日志进行备份，并且每周对审计日志做一次全备份并异地保存。NETCA采取严格的物理和逻辑访问控制措施，防止所有的审计日志和记录被未经授权的浏览、修改、读取、删除等。

5.4.6 审计日志的采集

NETCA 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

NETCA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NETCA保留进一步追究责任的权利。

5.4.8 脆弱性评估

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。NETCA认证（安全）策略管理委员会指定专业人员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，NETCA每年进行一次信息安全的风险评估。

5.5 记录归档

5.5.1 归档记录种类

NETCA归档的记录除了本文 5.4 所述的所有日志记录和数据库文件之外，还对以下几类事件进行归档记录，重要记录包括但不限于：

- 证书系统建设和升级文档；
- 证书和证书撤销列表；
- 证书申请支持文档，证书服务批准和拒绝的信息，与证书订户的协议；
- 审计记录；
- 证书策略、电子认证业务规则文档；
- 员工资料，包括但不限于背景调查、录用、培训等资料；
- 各类外部、内部评估文档。

5.5.2 档案保存期限

面向企事业单位、社会团体、社会公众的电子政务电子认证服务，NETCA的档案保存期限为档案相关证书或密钥失效后不低于五年；面向政务部门的电子政务电子认证服务，NETCA的档案保存期限为档案相关证书或密钥失效后不低于十年。

5.5.3 档案的保护

NETCA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

NETCA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。

5.5.5 档案的标识

对于每一个NETCA的档案，都给予适当标识，标识的内容包括：编号、归档时间、档案内容、档案管理员等。

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

5.6 CA 的密钥更替

在根证书到期以前，NETCA 将提前对根密钥进行更新。为了保证根密钥的更替不影响认证机构的正常运行，NETCA 将采取以下的方式进行：

1、由加密设备产生新的根证书的密钥对。

2、在更换密钥时签发三张根证书：

- 使用新的私有密钥对旧的公钥签发证书
- 使用旧的私有密钥对新的公钥签发证书
- 使用新的私有密钥对新的公钥签发证书

通过以上三张证书在一定阶段内的并存，达到密钥更替的目的，保证订户和依赖方能可靠地验证 NETCA 的根证书以及确保证书信任链的有效性。

NETCA 将在根证书到期前的五年，停止使用此证书对应的根密钥签发下级证书，并启用新的根证书对应的根密钥签发证书。

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，NETCA 将立即进行密钥更替：

- 密钥对已经被泄漏、被窃取、被篡改或者其它原因导致的密钥对安全性无法得到保证；
- 国家相关主管机构对密钥算法、密钥长度等有变更规定。

国家根CA密钥的更替策略与方式，以国家根CA主管部门公布的策略为准，NETCA不做详细描述。

5.7 损害和灾难恢复

5.7.1 NETCA 遭攻击或发生损害事故时的恢复程序

NETCA备份所有CA运行所需的数据、软件、CA密钥和资料，当发生事故或受到攻击时，用于系统的复原。NETCA制定相关的安全事件诊断和处理程序，包括事故处理、紧急应变、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、软件、数据被破坏或发生重大故障的事件；或NETCA下属注册机构因事故终止服务；或NETCA的CA密钥出现损毁、遗失、泄露、被破解、被篡改，

或者有被第三者窃用的怀疑时，NETCA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NETCA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，NETCA启动应急事件处理程序，由NETCA认证（安全）策略管理委员会和相关的专家进行评估，制定行动计划。如果需要撤销CA证书，会采取以下措施：

- 发布证书撤销状态到证书库；
- 在NETCA网站或其它通信方式发布关于撤销CA证书的处理通报；
- 重新更新CA密钥并签发新的CA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，NETCA启动灾难应急处理程序，异地恢复CA系统的运行。

NETCA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，NETCA会暂停业务受理，但证书及状态查询可以在24小时内恢复。

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

NETCA将努力寻找适合承接的认证机构，并在暂停或终止业务前九十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六十日前向工业和信息化部报告。不能就业务承接事项做出妥善安排的，将向工业和信息化部提出安排其它认证机构承接业务的申请。

无论如何，NETCA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，NETCA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NETCA，并通告其所办理证书的订户。

NETCA将作出妥善的安排，由其它注册机构或新设注册机构承接其业务，尽量减少对CA及证书订户的影响。

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

第 6 章 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

NETCA及其RA、订户的所有密钥对，都是由国家密码主管部门认可的密码设备或模块生成。

NETCA根密钥对及其下级CA密钥对的生成，是在预设定的程序下，由至少3名密钥管理员及1名监督人员参与下产生，并对每个环节进行记录和签名。

订户的签名密钥对由其持有的密码设备或模块产生，而加密密钥对由KMC的密码设备产生。

6.1.2 私钥的传递

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

订户的签名私钥在订户的密码设备或模块生成并保管；而订户的加密私钥在KMC产生后，通过安全通道传递回订户对应的密码设备或模块中，保证传递中间环节加密私钥不泄露。

6.1.3 公钥的传递

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

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

6.1.4 密钥长度

密钥算法和长度符合国家密码主管部门的规定。

6.1.5 密钥用法

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

NETCA的签名密钥用于签发下级CA、订户证书和CRL。

RA的签名密钥用于确认RA所做的审核证书等操作。

订户的签名密钥用于提供网络安全服务，如信息在传输过程中不被篡改、接收方能够通过数字证书来确认发送方的身份、发送方对于自己发送的信息不能抵赖等。订户的加密密钥用于对需在网络上传送的信息进行加密，保证信息除发送方和接受方外不被其他人窃取、篡改。

更多与协议和应用相关的密钥使用限制请参阅X.509标准中的密钥用法扩展域。

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

NETCA认证系统使用国家密码主管部门认可的密码产品，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

NETCA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。

NETCA使用国家密码主管部门认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5，N至少为3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

NETCA的根和下级CA的私钥不进行托管，其它的签名私钥也都不进行托管。

根据国家相关法规的要求，NETCA代订户向KMC申请加密密钥对的托管，其服务和安全保证参见本文 4.13 的内容。订户的签名私钥自行管理，以保证其不可否认性。

6.2.4 私钥备份

NETCA的私钥按本文 6.2.2 的管理方式备份到安全介质中（如IC卡或电子密匙），以作灾难恢复或密码设备更换时的恢复。

除本文 6.2.3 的托管服务外，NETCA不对订户的私钥进行备份。

6.2.5 私钥归档

NETCA对过期的CA密钥对进行归档。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NETCA与订户的协议，KMC可对不再托管的私钥进行归档。

6.2.6 私钥在密码模块中的导入和导出

NETCA的根CA及其下级CA的私钥可以在密码模块中导出，以实现私钥备份；NETCA的根CA及其下级CA的私钥，也可以导入到其它由国家密码主管部门认可的密码模块中，以实现灾难恢复和密码设备更新等。

订户可以使用NETCA提供的电子密匙，使其私钥无法从电子密匙中导出，确保订户私钥的安全；但订户的加密私钥可以导入到电子密匙中。订户也可使用由国家密码主管部门认可的其他密码设备或模块中。

6.2.7 私钥在密码模块中的保存

私钥在密码模块中是以密文的形式保存。

6.2.8 私钥的激活

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

订户的私钥保存在电子密匙或智能卡中，或其他由国家密码主管部门认可的密码设备或模块中，需要提供PIN码或指纹才能激活私钥。部分密码设备或模块的私钥激活可配置成一定周期后自动失效（停止）。

6.2.9 私钥的停止

所有硬件密码模块断电后或从接口中拔出或退出激活的应用软件后，私钥的激活状态将自动停止（取消激活）。NETCA的私钥还可采用本文 6.2.2 的控制方式进行停止。

停止状态下私钥仅以密文的形式存在。

6.2.10 私钥的销毁

NETCA对归档期过后的私钥进行销毁，包括保存在加密模块的中的副本及其使用备份，NETCA确保这种销毁是不可复原的。NETCA采用本文 6.2.2 的控制方式销毁密码模块中的私钥。

NETCA对从订户中回收的电子密匙或智能卡等密码设备或模块进行私钥销毁。订户在停止使用证书加解密功能的情况下，为防止密钥泄漏及可能发生的密钥盗用情况，也可以通过私钥的删除等方式销毁私钥。

6.3 密钥对的其它管理

6.3.1 公钥归档

NETCA和NETCA订户的公钥会被归档在数据库中。

6.3.2 密钥对与证书的有效期

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

在证实仍由原主体拥有并安全情况下，NETCA可以继续用原密钥对为该订户更新证书。

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。

NETCA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NETCA产生，或是预制的，或是由计算机随机产生的。

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一般使用密码信封或其在线生成，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。

NETCA在任何时候发现其激活数据可能泄露的情况下，对激活数据进行更改，并销毁存在的记录，不对历史激活数据归档。

订户应自行评估其密码设备或模块的PIN码的泄露情况或其他密码模块的访问控制风险。建议订户定期更换PIN码。

6.5 计算机和网络安全控制

6.5.1 计算机和网络安全性要求

NETCA用于运行认证系统和处理数据的生产用计算机由NETCA的系统维护人员维护，只有系统维护人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。

NETCA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。

NETCA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，系统维护人员定期更改这些口令。

NETCA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，并部署有入侵防御系统。

NETCA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。

NETCA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。

NETCA定期进行包括计算机和网络安全在内的整体评估。

6.6 生命周期技术控制

6.6.1 系统开发控制

NETCA的认证系统已获得《商用密码产品认证证书》，符合国家的相关标准和规范。

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

NETCA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安全性审查后启用。

6.6.2 系统改进控制

NETCA对认证系统生命周期内的任何补丁和升级版本进行控制；NETCA在安装系统补丁或系统升级之前对代码进行验证，包括测试和版本核对。

6.6.3 安全管理控制

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

6.7 网络安全性控制

NETCA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，并配置入侵防御系统，与防火墙联动。CA与RA的功能模块之间的通信采用VPN或其它安全通信协议连接，并采用安全身份认证技术。

NETCA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。只有网络维护人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，网络维护人员定期更改这些口令。

6.8 数字时间戳

NETCA在CA系统中部署时间服务器，该时间服务器采用的是国际标准时间（UTC），通过卫星定位系统得到。

CA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。

NETCA还提供数字时间戳（DTS）服务，符合RFC 3161标准。

第 7 章 证书、CRL 和 OCSP

7.1 证书

NETCA颁发的证书符合《GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式》、《GM/T 0015-2023数字证书格式》标准要求，并兼容ITU-T X.509和RFC 5280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

NETCA证书支持的标准扩展包括：

- 密钥用法（KeyUsage）
- 证书策略（Certificate Policies）
- 主体替换名称（Subject Alternative Names）
- 基本限制（Basic Constraints）
- 扩展密钥用法（Extended Key Usage）
- 证书撤销列表分发点（CRL Distribution Points）
- 颁发机构密钥标识符（Authority Key Identifier）
- 主体密钥标识符（Subject Key Identifier）
- 机构信息访问（AuthorityInfoAccess）

NETCA也支持GB/T 20518-2018标准及电子政务数字证书格式标准中指定的标准扩展，并支持用户自定义扩展，可根据用户或应用的要求定制。自定义扩展一般情况下为非关键项[4]。

应用如果遇到不能正确识别的关键证书扩展，则不应该接受此证书。

7.1.3 算法 OID

符合国家密码主管部门批准的算法对象标识符。

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 的要求，由DN表示。

另外，NETCA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可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。

[4] NETCA 不会随意增加自定义扩展项，而会综合评估证书应用范围和依赖方的可能状况做出决定。

7.1.5 证书密钥用法

NETCA 根据国家密码管理局的相关要求，严格规定数字证书的密钥用法。NETCA签发的数字证书中都在密钥用法（KeyUsage）中明确指明了此已认证的公开密钥可用于何种用途。订户和依赖方必须根据证书的密钥用法严格控制数字证书的使用场景。

7.1.6 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。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。订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NETCA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NETCA相关CPS的URL。

7.2 CRL

NETCA发布的CRL符合《GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式》、《GM/T 0015-2023数字证书格式》及ITU-T X.509、RFC 5280标准规范。

7.2.1 版本号

CRL版本号为X.509 V2。

7.2.2 CRL 和 CRL 条目扩展项

NETCA发布的CRL中，包含了以下扩展项：

- 颁发机构密钥标识符（Authority Key Identifier）
- CRL编号（CRL Number）

如果有明确的被撤销的原因，CRL条目则会包含被撤销的原因扩展(Reason Code)。

应用如果遇到不能正确识别的关键的CRL扩展或者CRL条目扩展，则不能使用该CRL来验证证书的撤销状态。

7.3 OCSP

NETCA采用OCSP提供在线证书状态查询服务。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，方便订户和依赖方及时的获取证书状态信息。

NETCA在撤销每一个证书后，由指定的OCSP响应者生成该证书的OCSP响应。NETCA OCSP响应符合RFC 6960格式标准，请求者可通过http承载协议向NETCA请求OCSP响应。NETCA OCSP响应包含证书的状态、状态最新变化时间、响应签发时间等信息。

7.3.1 版本号

OCSP版本号为 V1。

7.3.2 OCSP 扩展项

支持Nonce扩展。

第 8 章 认证机构审计和其他评估

NETCA建立内部审计机制，并组织信息安全风险评估活动。NETCA还接受国家电子认证服务主管部门组织的年度审查。在颁发粤港互认证书业务期间，接受粤港电子签名证书互认试点工作组安排的独立第三方机构的审查。其它第三方的外部审计或评估依据客户协议或其它政策进行。

8.1 审计的依据

审计是为了检查和监督 NETCA 及其下属机构或其它关联机构是否按照 NETCA CP 和相关 CPS、管理制度、安全策略等情况开展业务，以达到规避经营风险、提高服务质量、保障客户权益的目的。

8.2 审计的形式

审计分为外部审计与内部审计。

外部审计是由法律规定的主管部门、主管部门委托的第三方机构或 NETCA 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 NETCA 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

NETCA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、客户反馈异常、重大的系统变更等。

NETCA还接受国家电子认证服务主管部门组织的审查等。

8.4 审计或评估人员的资质

NETCA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NETCA认证（安全）策略管理委员会任命。

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 NETCA 的关系

NETCA内部审计人员要求与被审计对象无责任关系，为NETCA雇员。

NETCA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NETCA雇员，也可以是非NETCA雇员。

外部审计或评估人员应为与NETCA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

NETCA内部审计或评估涉及的内容包括以下：

- 人员管理
- 物理环境建设及安全管理
- 系统结构及其运行管理
- 密钥管理
- 客户服务规范管理
- 综合运营规范（如法规、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，NETCA将根据审计或评估报告制定和实施纠正措施，并由NETCA认证（安全）策略管理委员会监督执行。

对于重大的安全隐患，NETCA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

NETCA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，NETCA一般不公开审计或评估结果。

第 9 章 法律责任和其它业务条款

本章内容根据需求参见对应的网证通电子认证业务规则（CPS）或网证通电子政务电子认证业务规则（NETCA E-GOV CPS）。

第 10 章 支持服务管理

本章内容根据需求参见对应的网证通电子认证业务规则（CPS）或网证通电子政务电子认证业务规则（NETCA E-GOV CPS）。