网证通
NET CA

网证通电子认证业务规则

V5.3版

生效日期：2018年9月6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	2000 年	为初次提供电子认证服务编写。命名为《网证通认证业务操作规范》，试行版。
V2.0	2003 年 3 月 1 日	为符合《广东省电子交易条例》而修订。
V3.0	2005 年 7 月 20 日	为符合《中华人民共和国电子签名法》而修订。更名为《网证通认证业务声明》。
V4.0	2007 年 6 月 1 日	为更符合《电子认证业务规则规范（试行）》而重新编写，并修订错误描述。更名为《网证通电子认证业务规则》。
V4.1	2011 年 5 月 1 日	对订户的定义、初始身份确认、火灾预防和保护、CA 业务终止、注册机构业务终止等内容进行了修订。增加了证书变更操作规范、入侵侦测报警系统控制方法、证书密钥用法、审计依据等内容。更正了不规范名称的文字描述。
V4.2	2013 年 2 月 1 日	为符合《粤港电子签名证书互认证书策略》而修订，主要是补充了有关粤港互认证书的明确描述。
V4.3	2013 年 7 月 1 日	详细说明了“审计日志的备份”的具体操作方式，增加了归档记录种类列表的内容，将档案保存期限由五年改为十年，并详细说明了 OCSP 的操作方式及所提供的信息。
V4.4	2015 年 3 月 31 日	就 NETCA 增加 SM2 算法的根及相关证书格式标准、算法 OID、密钥长度等进行了描述；修订“3.2.3 个人的身份确认”，明确在签发满足《粤港电子签名证书互认证书策略》的数字证书时，“面对面审核查验证明其个人身份的原件”是 NETCA 必须采取的方式；对“4.11 订购结束”中“证书在有效期内被注销”的情形做出解释。
V4.5	2015 年 9 月 25 日	修改“1.4.1 适用的证书应用”中“机构证书”的适用范围定义;增加“3.2.2 机构的身份确认”中证照种类 ;修订“9.1.1 证书签发和更新费用”，明晰证书类型对应的市场售价范围。
V5.0	2017 年 5 月 2 日	增加支持多根的运营政策。修订和补充了相关章节，文章整体结构未作变化。主要根据 1.3.1 章补充，其他章节作相应的修订。并在兼容之前证书策略的前提下支持不同等级 CA 颁发证书的策略区分。增加了附录 A、B、C。
V5.1	2017 年 9 月 12 日	CCS NETCA Root L3 和 CCS NETCA Root L2 下各签发二级 CA，因此修订附录 B。
V5.2	2018 年 5 月 7 日	若干勘误，以及签发 SM2 L1 体系和 NETCA L3 Sub2 CA 而修订相关章节。

V5.3	2018 年 9 月 6 日	CCS NETCA Root L1 下签发二级 CA 以及添加扩展密钥用途自定义项，因此修订相关附录。

目　　录

第1章 概括性描述

1.1 概述

《网证通电子认证业务规则》（以下简称“NETCA CPS”）是广东省电子商务认证有限公司按照工业和信息化部《电子认证服务管理办法》的要求，依据《电子认证业务规则规范（试行）》制定。以规范广东省电子商务认证有限公司（以下简称“NETCA”[1]）的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 NETCA 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。

NETCA 按照《中华人民共和国电子签名法》及《电子认证服务管理办法》等法律法规要求，向公众提供电子认证服务。NETCA 认证体系内的成员包括有 NETCA（证书颁发机构，即 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，为订户提供网上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 NETCA CPS，并承担相应的责任。

随着数字证书应用的推广，NETCA 认证体系内建立和运营了多个根 CA，并对多个根 CA 进行不同等级的划分，以适应订户的不同的应用需求。同时，NETCA 也在国家根 CA 下运营了一个二级 CA。订户可以选择合适自己的根 CA 所签发的数字证书。

当前 NETCA CPS 版本在颁发证书策略 OID 为 1.3.6.1.4.1.18760.1.10、1.3.6.1.4.1.18760.20.10.3、1.3.6.1.4.1.18760.20.10.2 的证书时满足《中华人民共和国电子签名法》要求的一般性策略证书的颁发，该类证书可用于可靠性签名。同时，NETCA CPS 在颁发证书策略 OID 为 2.16.156.339.1.1.1.2.1 (自然人[2]) / 2.16.156.339.1.1.2.2.1 (法人[3])的证书（以下简称“粤港互认证书”）时亦满足《粤港电子签名证书互认证书策略》。

1.2 文档名称与标识

1.2.1 名称

本文档的名称是《网证通电子认证业务规则》，简称为 NETCA CPS，是 NETCA 在颁发证书过程中所采取的业务操作规则规范。之前的版本亦称为《广东省电子商务认证有限公司认证业务声明》，为指同一文件。

[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。
[2] “自然人”证书类型归属于“1.4 证书应用”中的“个人证书”。
[3] “法人”证书类型归属于“1.4 证书应用 ”中的“机构证书”。

1.2.2 版本

本 NETCA CPS 是 NETCA 发布的第十三个版本，当前版本号为 V5.3。

1.2.3 标识

NETCA CPS 的标识（OID）为：1.3.6.1.4.1.18760.12；其中 1.3.6.1.4.1.18760 为广东省电子商务认证有限公司的 OID。

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》及《电子认证服务管理办法》规定依法设立的电子认证服务机构（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、注销等一系列管理。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。

1.3.1.1 NETCA 的根

NETCA 建立的自有根包括以下五个：

序号	根 CA 名称	说明
1	NETCA Root ClassA	NETCA Root ClassA 是 NETCA 电子认证服务系统的 RSA 算法根的名称，甄别名为 CN=NETCA Root ClassA，O=NETCA Certificate Authority，C=CN，密钥长度为 RSA 2048 位，使用 SHA1WithRSAEncryption 签名算法签发证书，有效期为 30 年。
2	CCS NETCA Root L3	CCS NETCA Root L3 是 NETCA 电子认证服务系统的 RSA 算法根的名称，甄别名为 CN= CCS NETCA Root L3，O=NETCA Certificate Authority，C=CN，密钥长度为 RSA 4096 位，使用 SHA256WithRSAEncryption 签名算法签发证书，有效期为 20 年。

序号	根 CA 名称	说明
3	CCS NETCA Root L2	CCS NETCA Root L2 是 NETCA 电子认证服务系统的 RSA 算法根的名称，甄别名为 CN= CCS NETCA Root L2 ,O=NETCA Certificate Authority ,C=CN，密钥长度为 RSA 4096 位，使用 SHA256WithRSAEncryption 签名算法签发证书，有效期为 20 年。
4	CCS NETCA Root L1	CCS NETCA Root L1 是 NETCA 电子认证服务系统的 RSA 算法根的名称，甄别名为 CN= CCS NETCA Root L1 ,O=NETCA Certificate Authority ,C=CN，密钥长度为 RSA 4096 位，使用 SHA256WithRSAEncryption 签名算法签发证书，有效期为 20 年。
5	CCS NETCA SM2 Root L1	CCS NETCA SM2 Root L1 是 NETCA 电子认证服务系统的 SM2 算法根的名称，甄别名为 CN= CCS NETCA SM2 Root L1，O=NETCA Certificate Authority，C=CN，密钥长度为 SM2 256 位，使用 SM3WithSM2Encryption 签名算法签发证书，有效期为 30 年。

1.3.1.2 国家根下的独立运营 CA

序号	根 CA 名称	说明
-	ROOTCA（国家根 CA）	ROOTCA（国家根 CA）是 NETCA 电子认证服务系统加入国家根 CA 认证体系的根 CA 名称，甄别名为 CN=ROOTCA，O=NRCAC，C=CN，密钥长度为 SM2 256 位，使用 SM3WithSM2Encryption 签名算法签发证书，有效期为 30 年。
6	NETCA（二级运营 CA）	NETCA 为加入国家根 CA 认证体系的二级 CA 名称，甄别名为 CN=NETCA，O= NETCA Certificate Authority，C=CN，密钥长度为 SM2 256 位，使用 SM3WithSM2Encryption 签名算法签发证书，有效

		期为 20 年。

1.3.1.3 各 CA 的区别与划分

根据审核方式的不同，NETCA 将以上运营的五个 CA 分为 3 个等级：L3，L2 和 L1。他们的区别如下：

等级	差　　别
L3	严格的真实身份审核，包括面对面以及第三方数据库查核、单独调查等手段。
L2	依赖于经过评估的第三方身份审核（简称依赖审核方），评估要求基于真实的身份。比如在用的政府网上办事平台及其信息库。
L1	只通过单一渠道进行订户的身份审核。

各 CA 的对应等级如下：

序号	根 CA 名称	等级	说　　明
1	NETCA Root ClassA	L3	早期运营的 CA，其使用了 SHA1，今后不建议使用。
2	CCS NETCA Root L3	L3	-
3	CCS NETCA Root L2	L2	-
4	CCS NETCA Root L1	L1	-
5	CCS NETCA SM2 Root L1	L1	-
-	ROOTCA（国家根 CA）		详细情况参见国家根网站
6	NETCA（二级运营 CA）	L2	ROOTCA 下的二级 CA

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、证书注销、密钥恢复以及其他需要直接面向订户的业务，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 NETCA 的各

类数字证书以及数字证书存储介质。

RA 按照 NETCA 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 NETCA 的规定，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。

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

所有证书根据其颁发对象的不同，归为以下三种：

- 个人证书
- 机构证书
- 设备证书

NETCA 在开展业务时可能为某种对象的证书作特别的命名，但都会归属于以上的其中一种。

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 政府、企业、事业等机构所属人员	社会自然人或政府、企业、事业等机构所属人员在电子事务处理过程中，代表其身份，行使数字签名
机构证书	政府、企业、事业等机构	政府、企业、事业等机构在电子事务处理过程中，代表其身份，行使数字签名

证书类型	订户性质	适用范围
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

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 CPS 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

电话：(+8620)-38861746

电子邮件：CPS@cnca.net

1.5.3 CPS 批准流程

NETCA CPS 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[4])发布后，该 CPS 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 CPS。

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（安全）策略管理委员会指定专人负责版本控制及发布。

所有 CPS 相关公告和通知需获得认证（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 CPS 后向工业和信息化部备案。

[4] 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。

1.6 定义和缩写

1. CA（Certificate Authority）

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

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。

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. DTS（Digital Time Stamp)

数字时间戳服务的简称。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。

13. 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）。

14. 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.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它对象标识符。

15. 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。

16. 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。

17. 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。

18. 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。

19. 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。

20. 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。

21. 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。

22. 鉴别

辨别认定证书申请者提交材料真伪的过程。

23. 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。

24. 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《GM/T 0003-2012 SM2 椭圆曲线公钥密码算法》。

25. SM3 算法

中国国家密码管理局发布的密码杂凑算法。参见《GM/T 0004-2012 SM3 密码杂凑算法》。

26. 依赖审核方

NETCA 在受理数字证书申请时 ,其身份审核通过第三方已完成的程序替代，该第三方成为依赖审核方。通常为公众较为熟悉的相关政府部门或公众服务机构。

27. 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，NETCA CPS 最新的版本，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 签发的证书和证书注销列表（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注销的通知，而是准确描述上述内容。

NETCA 信息库将及时发布包括证书、CPS 的修订、证书挂起和注销的通知和其它资料等内容，这些内容保持与 CPS 和有关法律法规一致。

除 NETCA 授权者外，禁止访问信息库（或其它由 CA 或 RA 维护的数据）中任何被 CPS 和（或）NETCA 信息库宣布为机密信息的资料。

2.2 认证信息的发布

2.2.1 CPS 的发布

NETCA CPS 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 CPS 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，NETCA 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注销、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、注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。

2.3 发布时间或频率

2.3.1 CPS 的发布时间或频率

NETCA 将及时发布 CPS 的最新版本，一旦对规则的修改、补充、调整等获得批准，NETCA 将在 www.cnca.net 上发布，并将最新的 CPS 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 CPS 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 CPS，或者没有任何形式的公告、通知等形式宣布对 CPS 进行修改、补充、调整或者更新前，当前的 CPS 即处在有效的和正在实施的状态。

2.3.2 证书的发布时间或频率

数字证书在签发成功后，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 会在每批次挂起或注销证书后，在 4 小时内签发最新 CRL 并发布到 NETCA 的 LDAP 服务器或指定的信息库位置。从证书被挂起或注销，到反映该证书状态的最新 CRL 发布的最大延迟不超过 24 小时。并且不管如何，对于反映终端实体证书状态的 CRL 最长会在 7 天内重新签发一次，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、基于各种原因被注销、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、被注销、挂失/取消挂失时，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 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

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。

L3 和 L2 证书的 DN 所有项中内容都经过严格审核。L1 证书的 DN 通常为申请者能掌控的所标明的对象。

3.1.1 各类数字证书 CN 的取值方式

各类数字证书 CN 取值方式如下：

编号	证书类型	CN 取值方式
1	个人证书	个人姓名（与身份证明文件上标明的主体名称一致）
2	机构证书	机构名称[5]（与机构有效证件上标明的一致）
3	设备证书	域名、IP 地址、电子邮箱地址或其他实体标识，与申请者所属或能控制的设备地址/名称、账号名称一致

3.1.2 DN 说明条款

(1) DN 必须能明确标识订户的真实身份或其所属的设备地址/名称、账号名称；

(2) 单是主体名称不能唯一地标识客观实体；

(3) 应结合主体名称、电子邮箱、地址等信息，唯一标识客观实体。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

NETCA 为证书申请者提供电子密匙或其它符合要求的密码设备，用于生成

[5] 如果机构名称已在 O 中标注的话，CN 可能不再标注。

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订户手中。

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

证书申请者必需依据法律法规获取和使用密码。

3.2.2 机构的身份确认

NETCA 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。NETCA 通过面对面审核查验能证明其机构身份的证件的原件，或通过依赖审核方数据、或通过第三方信息数据或服务，或电话访问等 NETCA 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 NETCA 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。以面对面的审核方式确认授权代表身份时,通过核查法定的身份证明文件（包括但不限于身份证、护照或者其它身份证明资料），确认授权代表的真实身份。

一般需提供以下资料到 NETCA 或 NETCA 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：
   - 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
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
   - 其他有效身份证明资料

NETCA 在认为申请人的身份已经通过其它方式确认，则无需提交任何证件。是否需要提交及提交何种证件，NETCA 将在证书申请表或办理指引中予以明示。

若申请人提供的申请材料包括知识产权信息的，如包含商标信息，申请人必须提供知识产权注册文件或使用的许可证明文件，否则，身份审核不予通过。

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（包括依赖审核方原始数据、第三方平台数据、互联网访问等）鉴定订户身份及其声明的 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。

对于 L2 数字证书，其身份审核依赖于经评估和公布的第三方数据，NETCA

一般不再进行额外身份审核或确认。

对于 L1 数字证书，如果涉及机构身份，其审核只是关联主体标明资源的权属登记机构。

3.2.3 个人的身份确认

NETCA 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。NETCA 通过以下一种或多种的查验方式来确认个人身份，这些方式包括但不限于：

- 面对面审核查验证明其个人身份的原件
- 通过依赖审核方数据
- 通过第三方信息数据或服务
- 电话访问
- 其他 NETCA 认为恰当的方式

在签发满足《粤港电子签名证书互认证书策略》的数字证书时，NETCA 采用“面对面审核查验证明其个人身份的原件”审核用户身份。

一般情况下，个人申请者应提供以下资料到 NETCA 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 NETCA 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
   - 其他有效身份证明资料

NETCA 在认为申请人的身份已经通过其它方式确认 ,则无需提交任何证件。是否需要提交及提交何种证件 ,NETCA 将在证书申请表或办理指引中予以明示。

若申请人提供的申请材料包括知识产权信息的，如包含商标信息，申请人必须提供知识产权注册文件或使用的许可证明文件，否则，身份审核不予通过。

NETCA 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订户身份，申请人有配合业务受理员的调查工作的义务。

对于 L2 数字证书，其身份审核依赖于经评估和公布的第三方审核数据，NETCA 一般不再进行额外身份审核或确认。

对于 L1 数字证书，如果涉及个人身份，其审核只是关联主体标明资源的权属登记人。

3.2.4 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

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。所称的设备包括设备名称、域名地址、IP 地址、账号等。

NETCA 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订户身份及申请人对设备的拥有权，申请人有配合业务受理员的调查工作的义务。

3.2.5 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。

3.2.6 审核认证体系成员身份确认

1、 RA

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

2、 业务受理人员

- NETCA 的业务受理人员必须是 NETCA 或其所属 RA 机构的职员。
- 业务受理人员的身份除了必须符合个人证书申请者的条件外，还必须符合 NETCA 的相关规定。

3.2.7 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。如 NETCA 与其它 CA 进行了的相互认证，将在 NETCA 的网站中公布。

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，以不降低信任管理等级为标准。

3.2.8 依赖审核方的要求

NETCA 在 L2 的二级 CA 中将引入不同依赖方审核来替代 NETCA 的身份审核。这些依赖审核方的审核要求应与 NETCA 自身的身份审核要求相当。

NETCA 对依赖审核方的审核程序进行评估后引入，并跟踪其程序的变化及再评估。

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 证书注销请求中的身份鉴别

数字证书订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。

NETCA 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 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。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。

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。

NETCA 数字证书申请流程为：

1. 证书申请人从网上下载打印或从 NETCA 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 NETCA 的在线服务系统提交申请信息。
2. 按照本文 3.2 身份鉴别要求提交对应实体类型的证书申请表格及相关身份证明资料，到 NETCA 或其 RA 进行注册、身份审核和交费。

4.2 证书申请处理

4.2.1 身份审核

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，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。

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

- 网站公告或通知
- 在 RA 受理点面对面告知
- 电话通知
- 短信、电子邮件
- 其它与订户约定的方式

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. 订户获取数字证书及其密码信封；
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 CPS 和签署的协议。

1. 订户私钥的使用应符合证书中“密钥用途”（KeyUsage）的要求；
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、注销（若证书已到期或被挂起、注销，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 申请注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. 查验该证书没有被注销、挂起。

证书依赖方依据 NETCA 的相关保障措施，特别是不同的根及其等级，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，证书依赖方应参照 NETCA 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订户的行为，对于不符合证书或密钥用途的证书使用，依赖方可以拒绝接收。

4.6 证书更新

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. 证书将要到期或已到期或 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。

4.6.2 证书更新请求的处理

处理证书更新请求可以有以下两种方式：

1. 在线更新，只适合于证书未过期且未被注销的情形。即在证书即将过期前，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。L2 等级证书的在线更新可能受依赖审核方条件限制而有所不同，需关注 NETCA 网站信息。
2. 离线更新，一般情况下适合 L3、L2 等级证书更新情形。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。L2 等级证书的离线更新可能受依赖审核方条件限制而有所不同，需关注 NETCA 网站信息。

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. 因私钥泄漏而注销证书之后；
2. 证书到期且密钥也到期；
3. 订户或其授权代表提出证书密钥的更新申请；
4. NETCA 的策略要求或相关法律法规引致其它原因。

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。

L1 等级证书不适用于本条。

4.8.1 证书变更的情形

订户因其信息发生变化由其或其授权代表提出证书的变更申请。这些信息可以是：主体名称、主体身份 ID、所属机构、住址、电子邮件等。

4.8.2 证书变更请求的处理

订户或其授权代表提交证书变更申请表和身份证明材料 到 NETCA 或其 RA 进行证书变更。其身份鉴别方式除按本文 4.2 的要求外，需提供有效的变更证明文件。

如果涉及其证书内容变更的，则需要重新为订户制作新的证书。其处理方式同本文 4.2 的要求，同时注销原证书（参见本文 4.9 ）。

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. 证书变更后因注销原证书引起的 CRL 签发与发布同本文 4.9.5 。
4. 如果证书变更仅涉及非证书记载内容的变化，则 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 证书的注销和挂起

4.9.1 证书注销的情形

1. 证书密钥泄漏或存储证书的电子密匙丢失；
2. 证书主体名称列明的从属关系改变；
3. 证书主体的变更；
4. 任何与提供证书服务相关的协议到期；
5. 订户或其授权代表提出证书注销申请；
6. 订户违反 NETCA CPS 或签订的相关证书协议；

7. 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注销措施。

证书的注销既可以是订户提出申请，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注销。

4.9.2 证书注销的处理

在发生证书需注销的情形时，订户或其授权代表应及时填写证书注销申请表，并按本文 3.2 的要求携带身份证明材料，到NETCA或其RA进行申请。

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注销操作。

L1等级证书可以在线完成身份认证后直接注销。

当NETCA或其RA强制注销某一证书时，将在完成注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。

4.9.3 注销请求的宽限期

在发生需要注销证书的情形时，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进行注销登记，则需要通过电话挂失，先完成证书挂起。

4.9.4 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到NETCA或其RA进行注销时，可以先进行挂失，将证书挂起。

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，并确认申请人能正确回答证书申请时所登记的信息。必要时，受理人员可以再次通过已登记的联系方式再次确认。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 的身份审核要求到NETCA或其RA完成证书的注销申请或取消挂起的申请。若订户未在72小时内来NETCA办理注销手续的，NETCA将取消该挂起。

L1等级证书不适用于本条。

4.9.5 证书注销和挂起状态的发布

任何时候证书被注销或挂起，NETCA在30分钟内将该信息发布到NETCA信息库，并重新签发CRL。包含该注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。

当注销的证书过期或取消挂起时会被从下次发布的CRL中撤出。

4.9.6 依赖方检查证书状态的要求

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。

4.10 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。

4.11 订购结束

以下两种情况，表明证书订购结束：

1. 证书在有效期内被注销[6]；
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。

4.12 密钥生成、备份和恢复

4.12.1 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提供的电子密匙生成，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。

4.12.2 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：

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

密钥恢复服务根据KMC主管部门规定进行。

L1等级证书不适用本条款。

[6] 该情形指“4.9.1 证书注销的情形”描述的内容。

4.12.3 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提供的电子密匙产生的公钥对所申请（或恢复）的私钥进行加密传送，保持中间任何环节私钥都不会被获取。

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NETCA的规定要求执行。

5.1.2 物理访问

NETCA将功能区域按低到高划分为不同的四个安全等级，为接入区、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访问控制技术，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。

NETCA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双因素控制策略。

对于非业务管理和系统维护人员，只有获得NETCA认证（安全）策略管理委员会负责人批准，并在NETCA认证（安全）策略管理委员会授权的工作人员陪同下，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。

NETCA对监控记录的保存时间至少3个月；NETCA的门禁系统有进出时间记录和超时报警提示，NETCA定期对门禁记录进行整理归档，门禁进出时间记录的保存时间至少1年。

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. 客户服务人员
10. 运维工程师

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（见本文 5.1.2 ）；核心秘密（如CA根密钥）分管者和操作的物理访问控制者由不同的人员担任角色。

5.2.3 可信角色的鉴别

所有担任可信角色的人员需持有经授权的智能门禁卡（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NETCA可信人员背景调查管理的相关操作指南要求，对录用岗位的可信人员进行对应调查级别的背景调查，符合要求方予录用。可信人员背景调查至少包括以下方面：

- 学历、学位、职称
- 过往的就业情况

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

5.3.2 背景调查程序

拟录用担任信任角色的人员需同意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不定期进行可信人员背景调查，以便能够持续验证人员的可信程度和工作能力。

5.3.3 培训要求

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》及《电子认证

服务管理办法》、《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注销，所做的未授权操作将立即被注销失效。同时根据情节严重程度，对当事人作出相应处罚，包括内部处分、辞退、解雇等，涉及犯罪的将送司法机关处理。

5.4 审计日志程序

5.4.1 记录事件的类型

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

每个事件的记录至少包括以下信息：

- 发生的日期和事件
- 事件的内容
- 事件相关的实体
- 事件的标识

5.4.2 日志的处理周期

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，满足本文 5.5.2 要求的档案保存期限。

5.4.4 审计日志的保护

只有被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；
- 证书和证书吊销列表；
- 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

NETCA的档案保存期限至少为档案相关证书或密钥失效后10年。

5.5.3 档案的保护

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。在有效期未结束前，NETCA 将继续使用原有的根密钥签发 ARL，直到证书到期为止。

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。如果需要注销CA证书，会采取以下措施：

- 发布证书注销状态到证书库；

- 在NETCA网站或其它通信方式发布关于注销CA证书的处理通报；
- 重新更新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检测达到安全要求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电子密匙或其它密码设备产生，而加密密钥对由KMC的密码设备产生。

6.1.2 私钥的传递

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电子密匙或其它密码设备生成后随其实物通过离线方式传递到订户；而订户的加密私钥在KMC产生后，使用订户对应电子密匙或其它密码设备预生成的公钥加密后经过CA、RA传递回订户对应的电子密匙或其它密码设备中，保证传递中间环节加密私钥不泄露。

电子密匙或其它密码设备的离线传递，可以是CA或RA和订户面对面的交递，或采取密码信封保护方式发送（如邮递）给订户，或订户在线激活方式。

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

NETCA的RSA算法的根密钥长度及其下级CA密钥长度为2048位或4096位的RSA密钥对；NETCA的SM2算法的根密钥长度及其下级CA密钥长度为256位。

NETCA要求订户的RSA算法的密钥长度至少为1024位或2048位的RSA密钥对；NETCA要求订户的SM2算法的密钥长度为256位，否则证书申请不予批准。

NETCA要求凡符合《粤港电子签名证书互认证书策略》的订户的密钥对至少为2048位的RSA密钥，否则证书申请不予批准。

NETCA限制2048位RSA密钥对的根CA的使用，并逐步停用。NETCA限制1024位RSA密钥对的数字证书签发，建议用户转用SM2算法的数字证书。

6.1.5 公钥参数的产生

公钥参数由国家密码主管部门许可的设备或模块产生，NETCA不会专门安排其质量检查。

6.1.6 密钥用途

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

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标准中的密钥用途扩展域。

6.2 私钥保护与密码模块的控制

6.2.1 密码模块标准与控制

NETCA认证系统使用国家密码主管部门检测达到安全要求的密码产品，其密码模块符合国家规定的标准要求。其中CA的私钥保护达到《GM/T0028-2014》安全四级。订户的私钥保护达到《GM/T0028-2014》安全二级及以上，其中L3、L2等级证书建议订户达到安全三级或以上。

NETCA要求订户使用符合国家密码主管部门检测达到安全的密码产品。

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使用符合国家密码主管部门规定的安全标准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 4.12 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，保存期限按照本文 5.5.2 的要求。已归档的CA私钥不再利用，并在保存期过后进行销毁。

依据国家相关法规或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，也可以导入到其它满足国家密码主管部门规定的安全标准的密码模块中，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。订户也可使用经国家密码主管部门检测合格的达到安全要求的其他密码设备中。

6.2.7 私钥在密码模块中的保存

私钥在硬件密码模块中是以密文的形式保存。

6.2.8 私钥的激活

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，或其他满足安全等级的密码模块中，需要提供PIN码或指纹才能激活私钥。部分电子密匙或智能卡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进行私钥销毁。订户在停止使用证书加解密功能的情况下，为防止密钥泄漏及可能发生的密钥盗用情况，也可以使用NETCA提供的证书管理工具的删除功能销毁私钥。

6.3 密钥对的其它管理

6.3.1 公钥归档

NETCA和NETCA订户的公钥会随其证书作为NETCA安全运行数据被存放或被归档在第三方的数据库中，并在其失效后仍会在NETCA系统中保存至少5年。

6.3.2 密钥对与证书的有效期

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

对于保存在硬件密码模块的密钥对，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。

NETCA根证书有效期不超过30年，下级CA证书的有效期不超过25年，各根的有效期见本文 1.3.1.1。订户证书的有效期一般为1年-3年，最多为5年。

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。NETCA要求其业务人员或建议订户按以下规则设置或修改口令和PIN码：

- 长度不小于8个字符，除非系统或设备限制；
- 由数字、字母和特别符号（如“*&%$#@\~!”）组成；
- 不使用有含义的字串；
- 不能和操作员的名字相同；
- 不能包含用户名信息中的较长的子字符串；
- 不使用用过的口令或PIN码。

6.4.2 激活数据的保护

对于“秘密分享”，其持有者将遵守规定存放在具有物理保护的地方。

口令和PIN码只有授权的私钥使用人员才能知悉。需要传递的口令和PIN一般使用密码信封或其在线生成，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。

订户应自行评估其电子密匙的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的运维工程师维护，只有运维工程师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，运维工程师定期更改这些口令。

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定期聘请独立第三方机构进行包括计算机和网络安全在内的整体评估。

6.5.2 计算机的安全等级

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。

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。

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，并只有授权的工程实施人员才能访问；认证系统的重大升级需由NETCA认证（安全）策略管理委员会批准。

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。只有运维工程师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，运维工程师定期更改这些口令。

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，精度为秒。

第7章 证书、CRL 和 OCSP

7.1 证书

NETCA颁发的证书符合《GB/T 20518-2006 信息安全技术 公钥基础设施数字证书格式》、《GM/T 0015-2012基于SM2密码算法的数字证书格式规范》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（Key Usage）
- 证书策略（Certificate Policies）
- 主体替换名称（Subject Alternative Names）
- 基本限制（Basic Constraints）
- 扩展密钥用途（Extended Key Usage）
- 证书注销列表分发点（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、GM/T 0015-2012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[7]，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[8]。

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

对于RSA算法证书，NETCA在2012年以前设立的根使用SHA1WithRSAEncryption 算法签发证书 ,算法OID为 :1.2.840.113549.1.1.5。NETCA在2012年及以后设立的根使用SHA256WithRSAEncryption算法签发证书，算法OID为：1.2.840.113549.1.1.11

对于SM2算法证书，NETCA及国家根都使用SM3WithSM2算法签发证书，其算法OID为：1.2.156.10197.1.501。

[7] 更多扩展项请参见附录 A。

[8] 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。

SM2算法公钥，公钥标识为ECC椭圆曲线公钥密码算法，OID为1.2.840.10045.2.1，公钥参数中，标识ECC曲线为SM2椭圆曲线公钥密码算法，曲线OID为：1.2.156.10197.1.301。

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。

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（Key Usage）中明确指明了此已认证的公开密钥可用于何种用途。订户和依赖方必须根据证书的密钥用法严格控制数字证书的使用场景。

7.1.6 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。

NETCA 的证书策略 OID 为：1.3.6.1.4.1.18760.1.10 及 1.3.6.1.4.1.18760.20.10.X（具体如下表所示）。

证书等级	OID	说明
L3	1.3.6.1.4.1.18760.1.10 或 1.3.6.1.4.1.18760.20.10.3	早期颁发的证书属于L3，OID为1.3.6.1.4.1.18760.1.10
L2	1.3.6.1.4.1.18760.20.10.2	
L1	1.3.6.1.4.1.18760.20.10.1	

对于遵循《粤港两地电子签名证书互认办法》发放的数字证书，证书策略OID为：2.16.156.339.1.1.1.2.1 (自然人) / 2.16.156.339.1.1.2.2.1 (法人)。

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 CPS的URL，从中可以获取NETCA的《网证通电子认证业务规则》。

7.2 CRL

NETCA发布的CRL符合《GB/T 20518-2006 信息安全技术 公钥基础设施数字证书格式》、《GM/T 0015-2012基于SM2密码算法的数字证书格式规范》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）

如果有明确的被注销的原因，CRL条目则会包含被注销的原因扩展(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来验证证书的注销状态。

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在注销每一个证书后，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。

NETCA建议订户和依赖方及所关联的应用系统在条件允许的情况下优先采用OCSP。

7.3.1 版本号

OCSP版本号为 V1。

7.3.2 OCSP 扩展项

NETCA未使用OCSP相关扩展项。如果遇到OCSP响应返回unauthorized错误码、证书返回unknown状态或者不能正常识别的扩展，则应该使用其它的机制去验证该证书的状态。

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依据《中华人民共和国电子签名法》、《电子认证服务管理办法》、《网证通电子认证业务规则》，以及《粤港两地电子签名证书互认办法》（在提供相关业务的情况下）的要求，依法开展电子认证服务业务，以及在开展业务过程中，是否存在违反其它法律法规以及 NETCA 的业务规范、管理制度、安全策略等情况，以达到规避经营风险、提高服务质量、保障客户权益的目的。

8.2 审计的形式

审计分为外部审计与内部审计。

外部审计是由法律规定的主管部门、主管部门委托的第三方机构或 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。

国家电子认证服务主管部门组织的审查为每年一次。

粤港互认证书业务的审查为每年一次。

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

9.1 费用

9.1.1 证书签发和更新费用

NETCA对证书的签发、更新、密钥恢复和管理收取服务费用，在执行原广东省物价局《电子认证服务收费项目和收费标准》的文件基础上，结合数字证书的不同应用情况，NETCA不同种类的数字证书的具体费用将在服务协议或业务办理须知中告知。

9.1.2 证书查询费用

NETCA对发布到证书库中的所有证书查询不予收费。

9.1.3 证书状态信息查询费用

NETCA对发布到证书库中的CRL提供免费下载和使用服务。

NETCA的OCSP服务和其它定制的证书状态查询服务根据客户的服务协议要求进行收费。

9.1.4 其它服务费用

NETCA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，NETCA酌情收取费用。

9.1.5 退款政策

数字证书一旦发放，NETCA不办理退证、退款手续。

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

9.2 财务责任

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

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或依赖方不应承受的损失，NETCA根据CPS相关条款和国家相关法规进行赔付。

9.3 业务信息保密

9.3.1 保密信息的范围

NETCA列入保密的信息包括但不限于以下内容：

- 订户的个人信息和（或）机构信息；
- NETCA及其代理机构的证书业务处理信息；
- 所有的私钥信息；
- NETCA的运行数据和记录，以及保障运行的相关计划；
- NETCA与业务代理机构间的商业信息，包括商业计划、销售信息、贸易秘密和在非公开协议下从第三方得到的信息；
- NETCA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，NETCA没有义务公布或透露订户证书以外的任何信息；
- 其它书面或有形形式确认为保密的信息。

9.3.2 不在保密范畴内的信息

以下信息NETCA不列入保密范畴：

- 证书所载信息，以及证书状态信息；
- 由NETCA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，NETCA保留追究责任的权利。

9.3.3 保护保密信息的责任

NETCA及其业务代理机构、订户、关联实体等所有保密信息掌握者均有义务承担信息保密的责任。

NETCA执行严格的信息保密制度以确保只有经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。

当机密信息的所有者出于某种原因，要求NETCA公开或披露其所拥有的机密信息，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。

当NETCA在国家的法律法规要求下，或在法院的要求下必须披露本文 9.3.1 中的保密信息时，NETCA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，NETCA无须承担任何责任。

9.4 个人隐私保密

9.4.1 隐私保护方案

NETCA制定隐私保护策略，所有相关人员(包括NETCA及其RA的工作人员、订户等）必须严格遵守相应的规章制度。

NETCA根据国家相关法规的出台，及时调整隐私保护策略，以符合国家法规的要求。

9.4.2 作为隐私处理的信息

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

9.4.3 不被视为隐私的信息

所有在证书、CRL载明的订户信息不被视为隐私信息。

9.4.4 保护隐私信息的责任

NETCA对本文 9.4.2 所列的隐私信息进行保护，防止泄露。只有经NETCA授权的人员才能接触隐私信息，禁止任何未授权的访问、阅读或转移。

9.4.5 使用隐私信息的告知与同意

NETCA只在其业务范围内使用本文 9.4.2 所列的隐私信息，包括订户身份识别、管理、和服务的目的。这些使用，NETCA没有告知订户的义务，也无需得到订户的同意。

任何超出以上范围的隐私信息使用，需得到其本人的同意。对违法、违规使用、发布以上隐私信息的，NETCA承担由此造成的证书持有者、依赖方的损失，并负担相应的行政、经济责任。

9.4.6 依法律或行政程序的信息披露

当NETCA在国家的法律、规章的要求下，或在法院的要求下必须披露本文 9.4.2 中的隐私信息时，NETCA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，NETCA无须承担任何责任。

9.4.7 其他信息披露情形

当隐私信息其本人出于某种原因，要求NETCA公开或披露他的隐私信息，NETCA可根据授权或协议进行披露。如果这种披露行为涉及任何其他方的赔偿义务，NETCA不承担任何与此相关的或由于公开隐私信息引起的所有损失、损坏的赔偿责任。

9.5 知识产权

9.5.1 NETCA 自身拥有的知识产权声明

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，包括但不限于所有权、名称权和利益分享权等。

NETCA发行的证书及其状态信息，以及NETCA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NETCA，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。

9.5.2 NETCA 使用其他方知识产权的声明

NETCA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，NETCA保证都是合法的拥有相应权利。

订户或证书申请人声明并保证其交付给NETCA使用的网络域名、IP地址、主体名称及所有其它证书申请书的资料不得在任何管辖区域内干预或侵犯第三人的商标、服务标志、公司名称或其它知识产权等权利，而且不用于非法目的，包

括侵害、干扰协议或预期的商业利益、不公平竞争、损害他人信誉及干扰或误导他人。

9.6 陈述与担保

9.6.1 NETCA 的陈述与担保

NETCA的担保如下：

- 在批准证书申请和颁发证书中没有NETCA所知的或源自NETCA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NETCA所收到的信息保持一致。
- 除了未经验证的订户信息外,证书中的或证书中合并参考到的所有信息都是准确的。
- 签发给订户的证书符合本CPS的所有实质性要求。
- 按本CPS的规定，及时注销或挂起证书，并签发CRL。
- NETCA将向订户和依赖方通报任何已知的 ,将在根本上影响证书的有效性和可靠性的事件。

其它的陈述与担保参见与订户的服务协议。

9.6.2 RA 的陈述与担保

NETCA的RA担保如下：

- RA遵循NETCA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NETCA的服务标准和承诺。
- 在审核和批准证书申请中没有RA所知的或源自RA的错误陈述。
- 在处理证书申请时，保证足够检测和审核，使证书中的信息与RA所收到的信息保持一致。
- 除了未经验证的订户信息外，证书中的或证书中合并参考到的所有信息都是准确的。
- 签发给订户的证书符合本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挂起申请。

其它的陈述与担保参见与订户的服务协议。

9.6.3 订户的陈述与担保

订户的担保如下：

- 用与证书中所含公钥相对应的私钥所进行的每一次签名，都是订户自己的签名，并且在进行签名时，证书是有效的（没有过期、被挂起或注销）并已被订户接受。
- 订户的私钥得到很好的保护，未经授权的人员从未访问过其私钥。

- 订户在证书申请过程中向NETCA及其RA陈述的所有信息是真实的。
- 订户提供给NETCA及其RA用于申请证书的所有材料都是真实的。
- 如果存在代理人，那么订户和代理人两者负有连带责任。订户有责任就代理人所作的任何不实陈述与遗漏，通知NETCA其RA。
- 订户将按本CPS的规定，只将证书用于经过授权的或其它合法的使用目的。
- 订户的证书是终端证书。订户保证不将其证书用于发证机构所从事的业务，例如：把与证书中所含的公钥所对应的私钥用于签发任何证书（或认证其他任何形式的公钥）或签发CRL之类。

其它的陈述与担保参见与NETCA的服务协议。

9.6.4 依赖方的陈述和担保

依赖方的担保如下：

- 依赖方保证熟悉NETCA CPS以及和订户证书相关的证书政策，并了解和遵守证书的使用目的。依赖方确保证书及其对应的密钥对的确用于预定的目的。
- 依赖方在信赖订户的证书前，需收集足够的信息，判明是否NETCA签发的证书并在有效期内，根据最新的CRL检查证书的状态，查明证书是否还有效。
- 依赖方的信赖行为，表明其已同意本CPS的有关条款。

9.7 担保免责

NETCA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），NETCA 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NETCA签发的数字证书。
- 订户或依赖方没有使用可信赖系统进行证书操作。

- 订户在NETCA允许的目的范围之外使用或证书使用不当。

以上未尽事宜，依照中华人民共和国现行法律、法规执行。

9.8 NETCA 偿付责任及其限制

NETCA 的赔偿责任范围：

- 证书信息与订户提交的资料信息不一致，导致订户或依赖方直接损失。
- 由于 NETCA 的原因，致使订户或依赖方无法正常验证证书状态，导致订户或依赖方遭受损失。
- NETCA 仅在 NETCA 证书有效期限内承担以上损失或损害赔偿责任。

若 NETCA 违反本 CPS，NETCA 及其授权的发证机构，对于一份证书的所有当事人（包括但不限于订户、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 NETCA 改动。NETCA 声明的一份证书对所有该证书相关受损方法律赔偿责任之最高限额合计为该证书相应的服务费用的 10 倍。

9.9 订户和依赖方责任

订户和依赖方在使用和信赖证书时，如有任何行为或疏忽导致 NETCA 产生损失，则订户或依赖方应承担赔偿责任。

9.9.1 订户的赔偿责任情况

- 订户申请证书时，因故意、过失或者恶意提供不真实资料，造成 NETCA 或者其他方遭受损害的。
- 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知 NETCA 或其 RA，以及使用不安全系统或不当交付他人使用，造成 NETCA 或其他方遭受损害的。
- 订户提供使用的命名信息，包括但不限于名称、域名、IP、电子邮箱等，存在任何侵犯他人知识产权，造成 NETCA 或其他方遭受损害的。

9.9.2 依赖方的赔偿责任情况

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

9.10 有效期限与终止

9.10.1 有效期限

NETCA CPS自发布之日起正式生效。CPS中将详细注明版本号及发布日期。

9.10.2 终止

当新版本的CPS正式发布生效时，旧版本的CPS将自动终止。

9.10.3 效力的终止与保留

NETCA CPS一旦终止后，订户和依赖方原则上不受其条款的约束，但涉及知识产权和保密的相关条款继续生效。

9.11 对参与者的个别通告与沟通

除非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。

9.12 修订

9.12.1 修订程序

NETCA CPS由NETCA认证（安全）策略管理委员会根据情况进行审查，任何时候NETCA认证(安全)策略管理委员会认为有必要时即组织修订。修订后的版本经NETCA认证（安全）策略管理委员会审批后发布到NETCA网站（www.cnca.net），并报送工业和信息化部备案。

9.12.2 通告机制和期限

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

NETCA CPS的修改结果在NETCA的网站（www.cnca.net）上公布。

所有可能以书面形式提供给订户的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 NETCA 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。NETCA 也可以选择通过电子邮件（e-mail）向订户发送通知，该电子邮件地址在订户申请证书时已注明。

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

9.12.3 必须修改 CPS 的情形

如果出现下列情况，那么必须对CPS进行修改：

- 采用了新的密码体系或技术，并影响现有CPS的有效性
- 认证系统和有关管理规范发生重大升级或改变
- 法律法规的变化，并影响现有CPS的有效性
- 现有CPS出现重要缺陷

9.13 争议处理

如果NETCA与合作机构之间或与订户、依赖方之间发生争议，而当事人之间无法很好的解决出现的问题和争端，均提请广州仲裁委员会按照该会仲裁规则进行仲裁。仲裁裁决是终局的，对双方均具有约束力。

9.14 管辖法律

NETCA CPS在各方面按照中国现行法律和法规执行和解释，无论证书订户、依赖方等相关各方在何地居住以及在何处使用证书，本CPS的执行、解释和程序均适用中国法律，包括但不限于《中华人民共和国电子签名法》及《电子认证服务管理办法》、《电子认证服务密码管理办法》等。

9.15 与适用法律的符合性

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

9.16 一般条款

9.16.1 完整协议条款

NETCA CPS及NETCA的相关业务管理办法、国家相关法律法规构成NETCA的整体协议，各参与方的业务须遵循整体协议。

9.16.2 转让条款

若NETCA下属RA因故注销，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之所属订户须按国家规定，接受相应接管CA的证书服务条款。

9.16.3 分割性条款

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

9.16.4 强制执行条款

NETCA电子认证各参与方中，免除一方对合约某一条款违反应负的责任，不意味着免除这一方对其它条款违反或继续免除这一方对该条款违反应负的责任。

9.16.5 不可抗力条款

不可抗力，是指不能预见、不能避免并不能克服的客观情况。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；也可以是社会现象、社会异常事件或者政府行为。如合同订立后政府颁发新的政策、法律和行政法规，致使合同无法履行；再如战争、罢工、骚乱等社会异常事件。

在电子认证活动中，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。其他认证活动参与各方（如订户）不得就此提出异议或者申请任何补偿。

由于法律无法具体规定或者列举不可抗力的内容和种类，加上不可抗力本身的弹性较大，在理解上容易产生歧义，因而允许当事人在合同中订立不可抗力条款，根据交易的情况约定不可抗力的内容和种类。NETCA电子认证合同中的不可抗力条款可以在与数字证书申请表一起提供给订户的服务协议中规定，也可被规定在NETCA CPS中。

9.17 其它条款

9.17.1 各种规定的冲突

若NETCA CPS的规定与其它规定、指导方针或协议相互抵触，各参与方必须接受NETCA CPS的约束，除非

- NETCA CPS的规定为法律所禁止的范围内；
- 该冲突的协议的签署日期在NETCA CPS首次公开发行之前；
- 该冲突的协议明确地优于NETCA CPS。

9.17.2 安全资料的财产权益

除非另有约定，下列与安全相关的资料视为下列指定的当事人所拥有：

- 证书：证书为 NETCA 的产权所有。
- NETCA CPS：NETCA CPS 的版权为 NETCA 所有。
- 甄别名：甄别名为该命名实体（或其雇主或委托人）所有。
- 私钥：不论该密钥是以何种实体媒介存放或保护，私钥为合法使用或有权使用该密钥订户（或其雇主或委托人）所有。
- 公钥：不论该密钥以何种实体媒介存放或保护，公钥为订户（或其雇主或委托人）所有。
- NETCA 的私钥：NETCA 的私钥是 NETCA 的财产。这些私钥由 NETCA 授权分配和使用。
- NETCA 的公钥：NETCA 的公钥是 NETCA 的财产。NETCA 允许使用这些公钥。

9.17.3 损害性资料

证书申请人与订户不能把包含以下言论的任何资料提交给NETCA或其RA：

- 毁谤、中伤、不雅、色情、侮辱、迷信、憎恶或种族歧视的言论；
- 鼓吹非法活动或讨论非法活动，并试图从事此类活动的言论；
- 其它违法言论。

9.17.4 主管部门免责声明

在遵守本地法律监管要求和粤港电子签名证书互认证书策略的基础上，任何由于 NETCA 或相关证书的不足或疏忽所引起的责任和索偿，NETCA、订户和依赖方对粤港两地政府和电子认证服务主管部门免责。

附录A. 常用自定义扩展项

A.1. 用户证书服务号

此扩展项定义以证书为线索的订户服务跟踪，非关键扩展，定义如下：

Id- UserCertServiceId OBJECT IDENTIFIER ::= { 1 3 6 1 4 1 18760 1 14 }

UserCertServiceId ::= UTF8String

UserCertServiceID 由三部分构成，第一部分为用户服务号首部，由 16 个字节长的随机数的 HEX 编码构成，第二部分为分隔符@，第三部分为 CA 标识符。

A.2. 企业机构身份标识

此扩展项定义基于企业某种既有的 ID 而非名称的另一个标识 ,非关键扩展，定义如下：

```
Id-EnterpriseIdItems OBJECT IDENTIFIER ::= { 1 3 6 1 4 1 18760 1 15}
EnterpriseIdItems ::= IdentificationItems
IdentificationItems ::= SEQUENCE SIZE(1..MAX) OF IdentificationItem
IdentificationItem ::= SEQUENCE{
    type ItemType,
    encode ItemValueEncode OPTIONAL,
    value ItemValue
}
ItemType ::= INTEGER
ItemValueEncode ::= INTEGER
ItemValue ::= OCTET STRING
```

ItemType 表示证件类型。

ItemValueEncode 可选，表示证件值的编码方式，即原证件号经过何种编码。

ItemValue 标识证件号码编码后的值。

A.3. 个人身份标识

此扩展项定义基于个人某种既有的 ID 而非名称的另一个标识 ,非关键扩展，定义如下：

```
Id- IdentifyItems OBJECT IDENTIFIER ::= {1 3 6 1 4 1 18760 1 16}
IdentificationItems ::= IdentificationItems
```

IdentificationItems 参考 A.2 中的定义。ItemValueEncode 证件编码方式

只能使用加密的安全的编码方式，不能使用非安全的编码方式。

A.4. 前证书微缩图

此扩展项定义此证书更新前的证书微缩图（新申请证书不适用），非关键扩展，定义如下：

Id- NetcaCertThumbs OBJECT IDENTIFIER ::=
{ 1 3 6 1 4 1 18760 1 12 1 }
NetcaCertThumbs ::= SEQUENCE SIZE (1..MAX) OF NetcaCertThumb
NetcaCertThumb ::= SEQUENCE{
algorithm AlgorithmIdentifier,
thumbValue OCTET STRING
}

algorithm 表示前证书微缩图算法。
thumbValue 表示前证书微缩图的 HASH 值。

附录B. 体系结构

B.1. NETCA Root ClassA

NETCA Root ClassA 是 NETCA 电子认证服务系统的 RSA 算法根的名称，其下签发六个二级 CA[9]。

该体系各级 CA 证书的信息如下表：

CA 证书 DN 名称	证书序列号	签名算法及密钥长度	用途
CN = NETCA Root ClassA O = NETCA Certificate Authority C = CN	01	SHA1RSA 2048bit	签发二级 CA 证书
CN = NETCA Individual ClassA CA OU = Individual ClassA CA O = NETCA Certificate Authority C = CN	02	SHA1RSA 2048bit	签发个人证书
CN = NETCA Organization ClassA CA OU = Organization ClassA CA O = NETCA Certificate Authority C = CN	03	SHA1RSA 2048bit	签发机构证书/机构员工证书
CN = NETCA Server ClassA CA OU = Server ClassA CA O = NETCA Certificate Authority C = CN	04	SHA1RSA 2048bit	签发设备证书
CN = NETCA Secure E-mail ClassA CA OU = Secure E-mail ClassA CA O = NETCA Certificate Authority C = CN	05	SHA1RSA 2048bit	签发安全电子邮件证书
CN = NETCA Code Signing ClassA CA OU = Code Signing ClassA CA O = NETCA Certificate Authority C = CN	06	SHA1RSA 2048bit	签发代码签名证书
CN = NETCA Sub-1 ClassA CA OU = Sub-1 ClassA CA O = NETCA Certificate Authority C = CN	51 e5 2b 69 ab 7b 98 1f 6d b0 10 86 21 f6 b2 0f	SHA1RSA 2048bit	该二级 CA 证书带 CRLDP，签发个人/机构/设备等用户证书

B.2. CCS NETCA Root L3

CCS NETCA Root L3是NETCA电子认证服务系统的RSA算法根的名称，目前其下签发五个二级CA。该体系各级CA证书的信息如下表：

CA 证书 DN 名称	证书序列号	签名算法及密钥长度	用途
CN = CCS NETCA Root L3 O = NETCA Certificate Authority C = CN	40 b7 3f b5 71 74 88 43 49 03 83 22 9b 09 95 35	SHA256RSA 4096bit	签发二级 CA 证书
CN = CCS NETCA L3 Individual CA O = NETCA Certificate Authority	5f 75 a8 39 7b b3 92 59 fc 3a	SHA256RSA 2048bit	签发个人证书

[9] 二级 CA 将随着业务的发展会不断增多，请关注 NETCA 网站信息及时了解其新增的二级 CA。

CA 证书 DN 名称	证书序列号	签名算法及密钥长度	用途
C = CN	cf 08 01 b7 c0 2f		
CN = CCS NETCA L3 Organization CA O = NETCA Certificate Authority C = CN	4f 06 0d 73 fc 17 d9 4a f9 34 48 12 75 db 19 1a	SHA256RSA 2048bit	签发机构证书/机构员工证书
CN = CCS NETCA L3 Device CA O = NETCA Certificate Authority C = CN	53 a4 01 2e 3d c9 af a6 05 86 2c 8d b8 d0 9d 90	SHA256RSA 2048bit	签发设备证书
CN = CCS NETCA L3 Sub1 CA O = NETCA Certificate Authority C = CN	1d 0f 63 8d dc 76 e4 ef 87 51 16 ab 01 be 17 85	SHA256RSA 2048bit	签发个人/机构/设备等用户证书
CN = NETCA L3 Sub2 CA O = NETCA Certificate Authority C = CN	5f 9e 31 42 6d e4 ca 52 7c e8 ac dd 1b ce 8d 6d	SHA256RSA 2048bit	签发个人/机构/设备等用户证书

B.3. CCS NETCA Root L2

CCS NETCA Root L2是NETCA电子认证服务系统的RSA算法根的名称，其下签发三个二级CA。

该体系各级CA证书的信息如下表：

CA 证书 DN 名称	证书序列号	签名算法及密钥长度	用途
CN = CCS NETCA Root L2 O = NETCA Certificate Authority C = CN	08 bb dc 8a de c3 7d 7a 37 9c df 92 12 d8 2b d6	SHA256RSA 4096bit	签发二级 CA 证书
CN = CCS NETCA L2 Sub1 CA O = NETCA Certificate Authority C = CN	1c 8f ec 57 bf c4 58 ad ff 27 41 7b 8a e9 2f ea	SHA256RSA 2048bit	签发个人/机构/设备等用户证书
CN = CCS NETCA L2 Sub2 CA O = NETCA Certificate Authority C = CN	4a b2 ad 0d b9 77 ff e3 a3 99 19 db f8 a2 af b7	SHA256RSA 2048bit	签发个人/机构/设备等用户证书
CN = CCS NETCA L2 Sub3 CA O = NETCA Certificate Authority C = CN	6d 1a d3 5f c2 da 2d ce 82 5a 22 26 94 43 ad 94	SHA256RSA 2048bit	签发个人/机构/设备等用户证书

B.4. CCS NETCA Root L1

CCS NETCA Root L1是NETCA电子认证服务系统的RSA算法根的名称，目前其下签发两个二级CA。

该体系各级CA证书的信息如下表：

CA 证书 DN 名称	证书序列号	签名算法及密钥长度	用途
CN = CCS NETCA Root L1 O = NETCA Certificate Authority C = CN	08 31 63 f5 9e 96 f1 da d0 20 d3 40 72 62 d8 9f	SHA256RSA 4096bit	签发二级 CA 证书
CN = CCS NETCA L1 Sub1 CA O = NETCA Certificate Authority C = CN	22 9b 0f 2b 08 96 14 fb d6 ca d7 9b 96 52 13 b4	SHA256RSA 2048bit	签发个人/机构/设备等用户证书
CN = CCS NETCA L1 Sub2 CA O = NETCA Certificate Authority C = CN	27 3b f3 e0 f7 1c dd b7 a8 06 f6 d5 80 ca 1d a8	SHA256RSA 2048bit	签发个人/机构/设备等用户证书

B.5. CCS NETCA SM2 Root L1

CCS NETCA SM2 Root L1是NETCA电子认证服务系统的SM2算法根的名称，其下签发一个二级CA。

该体系各级CA证书的信息如下表：

CA 证书 DN 名称	证书序列号	签名算法及密钥长度	用途
CN = CCS NETCA SM2 Root L1 O = NETCA Certificate Authority C = CN	52 7a d8 3a 62 81 15 88 39 24 18 e7 e0 33 88 1e	SM3WithSM2 SM2 256	签发二级 CA 证书
CN = CCS NETCA SM2 L1 Sub1 CA O = NETCA Certificate Authority C = CN	1e 98 b9 5f e9 81 04 ed e3 66 9c a5 db 3c 96 46	SM3WithSM2 SM2 256	签发个人/机构/设备等订户证书

B.6. ROOTCA

ROOTCA是NETCA电子认证服务系统加入国家根CA认证体系的根CA名称，它为我司签发一个二级CA。

该体系各级CA证书的信息如下表：

CA 证书 DN 名称	证书序列号	签名算法及密钥长度	用途/备注
CN = ROOTCA O = NRCAC C = CN	69 e2 fe c0 17 0a c6 7b	SM3WithSM2 SM2 256	本文 1.3.1.2 所述的国家根 CA
CN = NETCA O = NETCA Certificate Authority C = CN	66 a1 af 8b 4b aa 97 6b a6 5d 20 30 84 29 bc 8e	SM3WithSM2 SM2 256	签发个人/机构/设备等订户证书

附录C. 数字证书格式模板

模版名称 / 模板格式		个人证书模版	机构证书模版	带组织名称的个人证书模版	设备证书模板
证书应用		个人证书	机构证书	个人证书	设备证书
版本号		V3	V3	V3	V3
证书序列号		有	有	有	有
颁发机构名称		CN、OU（可选）、O、C	CN、OU（可选）、O、C	CN、OU（可选）、O、C	CN、OU（可选）、O、C
密钥算法及长度		SHA256WithRSA 2048bit /SHA1WithRSA 2048bit /SM3WithSM2 256bit	SHA256WithRSA 2048bit /SHA1WithRSA 2048bit /SM3WithSM2 256bit	SHA256WithRSA 2048bit /SHA1WithRSA 2048bit /SM3WithSM2 256bit	SHA256WithRSA 2048bit /SHA1WithRSA 2048bit /SM3WithSM2 256bit
证书有效期		小于等于 5 年	小于等于 5 年	小于等于 5 年	小于等于 5 年
主体名称		E（可选）、CN、L、S、C	E（可选）、CN、OU（可选）、O、L、S、C	E（可选）、CN、OU（可选）、O、L、S、C	CN、OU（可选）、O（可选）、L（可选）、S（可选）、C（可选）
标准扩展	颁发机构密钥标识符	有	有	有	有
	主体密钥标识符	有	有	有	有
	证书策略	有	有	有	有
	主体替换名称	rfc822Name	无	rfc822Name	dNSName/iPAddress
	证书注销列表分发点	有	有	有	有
	机构信息访问	可选	可选	可选	可选
	基本限制	有	有	有	有
	密钥用法	digitalSignature/ nonRepudiation <L1 不设置>/ keyEncipherment/ dataEncipherment	digitalSignature/ nonRepudiation <L1 不设置>/ keyEncipherment/ dataEncipherment	digitalSignature/ nonRepudiation <L1 不设置>/ keyEncipherment/ dataEncipherment	digitalSignature/ keyEncipherment
	扩展密钥用途	(可选)	(可选)	(可选)	(可选)

模版名称 / 模板格式	个人证书模版	机构证书模版	带组织名称的个人证书模版	设备证书模板
自定义扩展	用户证书服务号 个人身份标识（可选） 前证书微缩图（可选）	用户证书服务号 企业机构身份标识（可选） 前证书微缩图（可选）	用户证书服务号 企业机构身份标识（可选） 个人身份标识（可选） 前证书微缩图（可选）	用户证书服务号 前证书微缩图（可选）

附录D. 扩展密钥用途自定义项

D.1. 电子发票

此项由网证通自定义，指明此密钥用于电子发票用途，定义如下：

id-elecInvoice OBJECT IDENTIFIER ::= {1 3 6 1 4 1 18760 11 12 12 2}

-- 密钥用法可以设置为 digitalSignature

（全文结束）