网证通
NET CA

广东省电子商务认证中心

电子认证操作规范(CPS)

版本 V2.0

2003年3月

www.cnca.net

广东省电子商务认证中心

Guangdong Electronic Certification Authority

目　录

第一章、 前言

1.1 概述

《广东省电子商务认证中心认证操作规范》（以下简称 CPS）由广东省电子商务认证中心（以下简称“广东 CA”）发布，明确规定广东 CA 在审批、签发、发布和废止[1]数字证书（以下简称证书）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。

广东 CA 认证体系内的成员包括有广东 CA、各业务 CA、CA 分中心、证书业务受理点（RA）、证书持有者、证书信赖者等成员，组成体系完整的广东 CA 电子认证架构，为用户提供互联网上的安全可靠的电子身份认证服务。

广东 CA 认证体系内的所有成员及广东 CA 各类证书持有者及使用者都必须严格遵循和执行该 CPS，并承担相应的责任。

1.2 认证体系的成员

1.2.1 CA 中心（Certification Authority)

广东 CA、各业务 CA 及其下属 CA 分中心统称为 CA 中心。

1.2.2 广东 CA

广东省电子商务认证中心，简称广东 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 为电子商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、废止等一系列管理。

[1]本文中废止的定义等同于撤销。

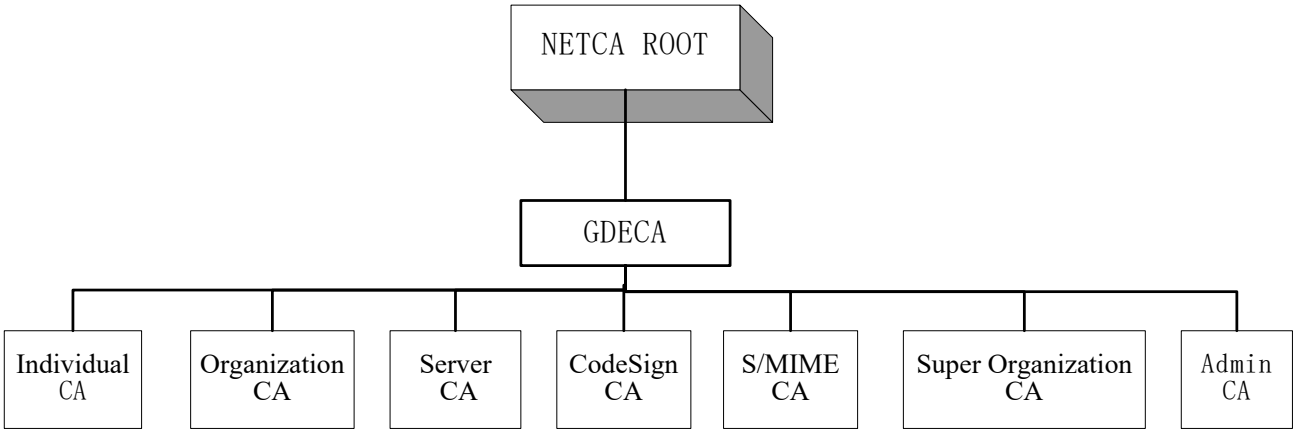

图 一-1 广东 CA 体系结构图

1.2.3 业务 CA

1.2.3.1 Admin CA

签发管理员证书及 CRL。管理员证书分为各类型 CA、RA 管理员证书，不同的证书对应于不同的管理权限，实行对 CA、RA 的有效分权管理监控。

1.2.3.2 Individual CA

签发个人证书及 CRL。个人证书是专门为个人用户提供的数字证书，以帮助个人用户在网络上表明身份、进行安全事务处理和安全交易操作。

1.2.3.3 Organization CA

签发单位证书和单位员工证书和 CRL。单位证书和单位员工证书是专门为单位或单位中的工作人员提供的数字证书，以帮助单位在进行公务或商业活动时，建立一个虚拟环境中的信任度。

1.2.3.4 Server CA

签发服务器证书和 CRL。服务器证书是签发给单位的服务器，与互联网中的服务器域名相对应，用来证明站点真实身份，提高信息数据的安全性。

1.2.3.5 CodeSign CA

签发代码签名证书及 CRL，为软件开发商提供对软件代码做数字签名的技术，可以有效防止软件代码被篡改，使用户免遭病毒与黑客程序的侵扰，同时可以保护软件开发商的版权利益。

1.2.3.6 S/MIME CA

签发安全电子邮件证书及 CRL，结合使用数字证书和 S/MIME 技术，对普通电子邮件做加密

和数字签名处理，确保电子邮件内容的完整性、机密性、发件人身份确认性和不可抵赖性。

1.2.3.7 Super Organization CA

签发 CA 分中心证书及 CRL。为适合用户不同的需求，签发特定的 CA 证书。

1.2.4 CA 分中心

CA 分中心是由 Super Organization CA 签发 CA，包括部门级、企业级、运营商级 CA 分中心，主要适用于各种规模企业内部使用。各企业可根据的实际情况，定制不同的功能、服务、可签发证书的用户量，最大程度上节省建立系统的时间和企业成本。证书的签发完全由 CA 分中心控制，无需再经广东 CA，方便企业运行相应的操作、控制。

1.2.4.1 部门级 CA 分中心

部门级 CA 分中心是专门为政府部门或中小型企业定制的可独立运行于内网的小型 CA。系统用户量在 5000 以下，主要为建有内部网络的政府部门、中小型企业在内部进行安全电子邮件发送、公文传递、网上办公等安全电子事务处理提供安全认证服务。

系统主要功能包括证书申请、证书管理、证书发布、证书更新或废止、证书查询下载、证书验证、发布 CRL 及支持多种审核策略。

1.2.4.2 企业级 CA 分中心

企业级 CA 分中心是专门为政府部门或大中型企业定制的可独立运行于内网的中型 CA 系统。系统用户量在 10 万以下，主要为建有内部网络的政府机构、大中型企业在内部进行安全电子邮件发送、公文传递、网上办公等安全电子事务处理提供安全认证服务。

系统主要功能包括证书申请、证书管理、证书发布、证书更新或废止、证书查询下载、证书验证、发布 CRL、支持多种审核策略及提供业务统计、系统监控、LDAP、OCSP 等服务。

1.2.4.3 运营商级 CA 分中心

运营商级 CA 分中心是专门为政府或大型企业定制的可独立运行于内网（专网）的大型 CA 系统。系统用户量高达两百万级，主要为建有大型专用网络的政府、大型企业在专网内进行安全电子邮件发送、公文传递、网上办公等安全电子事务处理提供安全认证服务。

系统主要功能包括证书申请、证书管理、证书发布、证书更新或废止、证书查询下载、证书验证、发布 CRL、支持多种审核策略及提供业务统计、系统监控、LDAP、OCSP、DTS、数据归档、交叉认证等服务。

1.2.5 数字证书业务受理点 （以下简称 RA：Registration Authority）

RA 的业务范围包括：代理用户注册管理业务和销售数字证书产品业务。其中用户注册管理业务是指受理用户的证书申请、审核用户身份、批准证书申请、证书制作、发放证书、接受和处理证书更新、证书废止，以及其他需要直接面向用户的业务。销售数字证书产品业务是指销售广东 CA 的各类数字证书以及数字证书存储介质。

RA 应按照广东 CA 制定的《认证业务操作规范》、《数字证书管理制度》及《数字证书代理业务管理办法》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，应按照广东 CA 的规定，使用统一的品牌和标志，执行统一的资费标准，向用户提供统一标准的服务。

1.2.6 证书持有者

证书持有者是指持有广东 CA 颁发的各类证书且持有与列示于证书中的公钥相对应的私钥的人、物对象或单位组织。简单地说，证书持有者，也就是证书用户，包括个人、企业、团体、提供网上服务或享受网上服务的实体和应用服务器等。

1.2.7 证书信赖者

一般而言，信赖即为一种假设的关系，相信对方的行为将合于所预期。信赖有其特定的功能。在证书认定的架构下，它主要是用于描述鉴别实体（即证书信赖者）与广东 CA 之间的信任关系。证书信赖者可以理解为行为上信任并依赖所收到的证书及电子签名的一方。简单地说，证书信赖者就是指信赖数字证书的人或单位。

1.2.8 其他成员

NETCA 认证体系的相关其他成员。

1.3 证书的适用范围

证书类型	用户性质	适用范围
个人证书	社会自然人	社会自然人在电子政务、电子商务过程中，代表其身份，行使电子签名
单位证书	政府、企业、事业单位或其下属部门	政府公务员、企业、事业单位的员工在电子政务、电子商务过程中，代表其身份，行使电子签名

证书类型	用户性质	适用范围
单位员工证书	政府公务员、企业、事业单位的员工	政府、企业、事业单位或其下属部门在电子政务、电子商务过程代表其身份，行使电子签名
服务器证书	政府、企业、事业单位或其下属部门所属的服务器	政府、企业、事业单位或其下属部门所属的在电子政务、电子商务过程代表其服务器身份
代码签名证书	政府、企业、事业单位或其下属部门 社会自然人	政府、企业、事业单位或其下属部门在电子政务、电子商务过程代表其身份，行使电子签名
安全电子邮件证书	合法 Email 地址持有者	安全电子邮件系统

表格 1 各类证书适用范围表

1.4 政策管理

CPS 由广东省电子商务认证有限公司管理委员会制定，版权由广东省电子商务认证有限公司完全拥有。在广东 CA 证书政策和操作规范做出任何变动之前，广东 CA 管理委员会将对提供的变动建议进行研究，做出变更决定。在征询广东 CA 律师有关法律方面的意见后，形成决议。

广东 CA 将在决议形成后，在广东 CA 网站公布变更后的 CPS 正式文档。

广东 CA 将对 CPS 进行严格的版本控制，由广东 CA 管理委员会指定专人负责。

所有公告和通知获广东 CA 进行数字签名后，将在广东 CA 网站（Http://www.cnca.net）上公布。

第二章、 信息发布

2.1 CPS 的发布

《广东省电子商务认证中心电子认证操作规范》版权由广东 CA 拥有，并负责本规范的解释，一经广东 CA 在网页 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 CA 核准和发布。有需要人士可访问广东 CA 网页 www.cnca.net 查看本规范，对具体个人不另行通知。

2.2 广东 CA 公众信息的发布

广东 CA 在 www.cnca.net 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，确保只有授权的广东 CA 工作人员才能编写、修改和删除广东 CA 在线发布的信息资料。同时广东 CA 在必要时可自主选择是否实行信息的权限管理，以确保只有数字证书用户才有权阅读受广东 CA 权限控制的信息资料。

2.3 数字证书的发布

数字证书在签发成功后，广东 CA 将发送邮件通知证书用户下载证书，同时自动将该证书复本发布到证书存储区。广东 CA 定期公布在证书有效期内被废止的数字证书。证书用户都可以在广东 CA 的目录服务中查询获得有关信息。

广东 CA 的目录服务器上每日更新目录，每工作日人工发布最新 CRL。证书用户可在广东 CA 网页 www.cnca.net 查询、下载数字证书、CRL、增量 CRL 和分块 CRL。

如有需求，证书用户可向 RA 申请通过介质载体，以离线方式获得数字证书。

第三章、 身份审核

3.1 主体名称

每张数字证书的主题中都包含一个主体名称（CN），目的是标识证书持有者的身份。

3.1.1 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。

3.1.2 各类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.	单位证书	单位名称（与营业执照等有效证件上标明的一致）
3.	单位员工证书	单位员工的姓名（与其身份证上标明的一致）
4.	代码签名证书	单位名称（与营业执照等有效证件上标明的一致）
5.	服务器证书	域名或者 IP 地址
6.	安全电子邮件证书	匿名，只提供电子邮件地址

表格 2 证书的主体名称命名方式

3.2 证书申请

3.2.1 审核单位身份

3.2.1.1 广东 **CA** 的单位证书、单位员工证书、服务器证书、代码签名证书只提供给单位或部门性质的申请者，不对个人用户提供该项服务，因此，在审批申请信息时，必须审核单位的身份。

3.2.1.2 单位申请者填写书面申请表（一式三份），经过单位授权代表的签署及单位盖章后，携带以下资料到广东 **CA** 或广东 **CA** 的其他业务受理点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单位盖章证明）：

a) 申请单位的组织机构代码证的复印件

b) 申请单位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) 事业单位登记证
4) 事业单位法人登记证
5) 税务登记证
6) 组织机构代码证
7) 社会团体登记证
8) 社会团体法人登记证
9) 人民团体登记证
10) 人民团体法人登记证
11) 政府批文
12) 其他有效证件

c) 经办人身份证原件与复印件

d) 书面申请表

e) 单位员工的身份证复印件（在申请单位员工证书的情况下）

3.2.1.3 广东 CA 或广东 CA 的其他业务受理点的审批人员认真、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。

3.2.2 审核个人身份

广东 CA 的个人证书签发给合法的个人申请者，广东 CA 需要审批个人申请者的身份。

3.2.2.1 个人申请者填写书面申请表（一式三份），个人签字后，携带以下资料到广东 CA 或广东 CA 的其他业务受理点进行身份审核及交费手续：

1) 个人身份证原件与复印件（或者是户口簿或护照）

2) 书面申请表（一式三份）

3.2.2.2 广东 **CA** 或广东 **CA** 的其他业务受理点的审批人员认真、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

CA 分中心、RA 管理员必须是广东 CA 的 CA 分中心或 RA 的正式职员。

3.2.3.1 **CA** 分中心、**RA** 管理员的身份除了必须符合单位员工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。

3.2.3.2 **CA** 分中心、**RA** 的资格由广东 **CA** 根据认证业务管理办法来审查批准。

3.2.4 CA 相互认证的标准

3.2.4.1 广东 **CA** 通过交叉认证、双向认证、证书交换中心等与其他认证中心建立相互认证的关系。

3.3 证书更新

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

3.3.2 广东 **CA** 也支持网上表单签名形式的证书更新身份审核。

3.3.3 个人申请者、单位申请者、安全电子邮件证书的申请者的更新申请审核办法有所不同：

申请者类型	审核要求
个人	方式一： 在广东 CA 的网站上用更新前的数字证书所对应的私钥对更新申请表进行签名确认。

申请者类型	审核要求
	方式二： 向广东 CA 或其下属业务受理点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
单位	方式一： 在广东 CA 的网站上用更新前的数字证书所对应的私钥对更新申请表进行签名确认。 方式二： 向广东 CA 或其下属业务受理点提交书面申请表及申请单位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单位有效证件副本的原件。
安全电子邮件证书用户	在广东 CA 的网站上用更新前的数字证书所对应的私钥对更新申请表进行签名确认。

表格 3 数字证书更新申请审核要求

3.4 证书废止

3.4.1 数字证书用户申请废止数字证书时，需要经过身份审核，才能够完成更新的过程。

3.4.2 个人申请者、单位申请者、安全电子邮件证书的申请者的废止申请审核办法有所不同：

申请者类型	审核要求
个人	向广东 CA 或其下属业务受理点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。
单位	向广东 CA 或其下属业务受理点提交书面申请表及申请单位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单位有效证件副本的原件。

申请者类型	审核要求
其他	在广东 CA 的网站上用废止前的证书所对应的私钥对废止申请表进行签名确认。

表格 4 数字证书废止申请审核要求

第四章、 证书操作规定

4.1 证书申请

4.1.1 申请流程

4.1.1.1 广东 CA 提供两种证书申请方式：流程一和流程二。

4.1.1.2 证书申请流程一

1) 用户在网上下载、填写书面申请表格。

2) 所有证书申请用户，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，到广东 CA 或其它业务受理点进行身份审核和交费，具体身份审核所需资料请参考 3.2 证书申请

3) 对于安全电子邮件的用户，因为安全电子邮件证书所保证的是用户的电子邮件地址，所以身份审核将通过电子邮件确认的方式进行，广东 CA 所提供的安全邮件证书对电子邮件之外的信息不进行审核。

4.1.1.3 证书申请流程二

1) 用户在网上提交申请表格，获得业务受理号。

2) 用户下载并填写书面申请表格（注意把上述获得的业务受理号填在书面申请表格相应的地方）。

3) 所有证书申请用户，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，到广东 CA 或其它业务受理点进行身份审核和交费，具体身份审核所需资料请参考 3.2 证书申请

4) 对于安全电子邮件的用户，因为安全电子邮件证书所保证的是用户的电子邮件地址，所以身份审核将通过电子邮件确认的方式进行，广东 CA 所提供的安全邮件证书对电子邮件之外的信息不进行审核。

4.1.1.4 广东 CA 支持用户在线申请证书，在安全性和认证得到认可的情况下，广东 CA 允许用户通过 Internet 提供用户的信息，无需亲自到广东 CA 或其它业务受理点提交

申请表格和身份审核资料。此类申请方式只适用于各类网上试用型证书，广东 CA 对其不承担任何责任。

4.1.2 审批流程

4.1.2.1 根据两种数字证书申请方式：流程一和流程二，业务受理点进行审批的过程也有针对性分为流程一的审批过程和流程二的审批过程。

4.1.2.2 流程一的审批过程：

1) 广东 CA 或其它业务受理点对用户提交的身份证明资料和书面申请表格进行初次审核和交费。

2) 对初次审核和交费者，证书受理员登录系统并根据用户提交的申请表格及交费情况，产生对应的业务受理号并录入用户资料，完成身份审批和交费审批操作。若以上操作成功，系统将自动发送一封通知邮件给用户。

3) 对于安全电子邮件，身份审核将通过电子邮件确认的方式进行，广东 CA 所提供的安全邮件证书对电子邮件之外的信息不进行审核。

4) 用户根据邮件提供的业务受理号及密码登录网站，按步骤完成网上申请手续。

5) 对于安全电子邮件用户，要响应身份审核邮件。

4.1.2.3 “流程二”的审批过程：

1) 广东 CA 或其它业务受理点对用户提交的身份证明资料和书面申请表格进行初次审核和交费。

2) 初次审核和交费通过者，证书受理员进入 RA 系统并根据用户提交的申请表格及交费情况，进行身份审批和交费审批操作。操作成功，系统自动发送一封通知邮件给用户。

3) 对于安全电子邮件，身份审核将通过电子邮件确认的方式进行，广东 CA 所提供的安全邮件证书对电子邮件之外的信息不进行审核。

4) 审批通过者，RA 系统自动发一封通知邮件给用户，用户根据邮件提供的业务受理号及密码登录网站，按步骤完成网上申请手续。

5) 对于安全电子邮件用户，要响应身份审核邮件。

4.1.3 签发流程

1) 对于审批通过的用户，广东 CA 在一个工作日内对其进行 CA 签发。

2) 在 CA 签发之前，受理员有权对用户进行二次审核，有权对认为身份审核不能通过的用户进行拒绝签发的操作。

3) 对于签发成功的用户，CA 系统自动发送一封通知邮件给用户，并提示用户下载安装数字证书。

4.1.4 证书使用

4.1.4.1 证书的签发：广东 CA 签发了证书后，用户可在第二个工作日上网下载安装证书，至此，用户就接收了证书。用户接收了证书后，必须妥善保存好证书对应的私钥。同时，用户可以通过广东 CA 的证书目录中下载个人或其它人的数字证书。

4.1.4.2 用户私钥和证书的用途：

编号	证书类型	用户私钥和证书的用途
1.	个人证书	用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用户的其他信息。 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.	单位证书	颁发给独立的单位、组织，在互联网上证明该单位、组织的身份。 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.	单位员工证书	单位员工证书对外代表单位中具体的某一位员工。 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。
4.	服务器证书	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。 主要用于：实现安全站点、配合个人证书、单位证书、

编号	证书类型	用户私钥和证书的用途
		单位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
5.	代码签名证书	为软件开发商提供对软件代码做数字签名的技术，可以有效防止软件代码被篡改，使用户免遭病毒与黑客程序的侵扰，同时可以保护软件开发商的版权利益
6.	安全电子邮件证书	用于实现安全电子邮件的通信方式

表格 5 用户私钥和证书的用途

4.1.4.3 证书及密钥的使用说明：数字证书的用户必须确保自己的私钥不被他人窃取。而数字证书和公钥则通过电子邮件、**www.cnca.net** 上下载等方式向他人公布。

4.1.4.4 他人证书和公钥的用途：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。

4.2 证书更新

4.2.1 证书更新的原因和用户类型

4.2.1.1 证书更新的原因

1) 原有证书的密钥泄漏
2) 证书操作终止
3) 原有证书有效期将到期
4) 其他原因

4.2.1.2 证书更新的用户类型：原有证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体，以及其他凡是广东 **CA** 各类证书的有效期限未到的证书持有者。

4.2.2 更新流程

4.2.2.1 方式一：产生新的密钥对和证书的更新方式

1) 用户在通过填写书面更新申请表格并交费，在获得广东 CA 或其它业务受理点允许的情况下，用户自行在广东 CA 的网站上进行更新操作。（用户必须拥有以前那张数字证书的业务受理号和密码才能进行更新操作）。

2) 用户在网站上进行更新操作时注意新证书请求的选择有两种，即重新选择 CSP 产生、选择用户自己产生的 CSP。

3) 用户选择证书请求后可进行表单的签名操作。

4) 更新申请提交成功后，系统返回一个新的业务受理号，并发送通知邮件给用户。

5) 用户把新的业务受理号通过可靠方法提供给广东 CA。

4.2.2.2 更新证书的发放和通知

1) 广东 CA 在获得用户更新后证书的业务受理号后，在 RA 端为用户进行交费审批。（由于用户已在更新操作时用旧的证书进行了签名，RA 端就无需再对用户的身份进行审批）

2) CA 签发证书。证书签发成功，系统会发送通知邮件给用户。

3) 用户根据通知邮件，在一个工作日后自行上广东 CA 的网站下载新证书。

4.2.2.3 方式二：新证书继续使用原有密钥对更新流程

1) 用户在通过填写书面更新申请表格并交费，在获得广东 CA 或其它业务受理点允许的情况下，用户自行在广东 CA 的网站上进行更新操作。（用户必须拥有以前那张数字证书的业务受理号和密码才能进行更新操作）

2) 用户在网站上进行更新操作时注意选择“使用原有的证书请求”并用原有的证书进行表单的签名操作。

3) 更新申请提交成功后，系统返回一个新的业务受理号，并发送通知邮件给用户。

4) 用户把新的业务受理号通过可靠方法提供给广东 CA。

4.2.2.4 更新证书的发放和通知

1) 广东 CA 在获得用户更新后证书的业务受理号后，在 RA 端为用户进行交费审批。（由于用户已在更新操作时用旧的证书进行了签名，RA 端就无需再对用户的身份进行审批）。

2) CA 签发证书。证书签发成功，系统会发送通知邮件给用户。

3) 用户根据通知邮件，在一个工作日后自行上广东 CA 的网站下载新证书。

4.2.3 更新注意事项

请用户在进行证书更新之前需要将加密邮件等加密文件进行解密，同时备份（例如将邮件内容拷贝以明文方式存储或将邮件附件保存），然后将证书删除。以上操作完成后才能进行证书的更新。

如因用户未解密文件而进行证书更新，由此造成的可能损失，广东 CA 概不负责。

4.3 证书挂失/取消挂失和废止

4.3.1 证书挂失

4.3.1.1 挂失的原因：当用户发现证书可能由私钥泄密或其它原因引起不可信时，要及时将证书挂失。

4.3.1.2 用户类型包括：原有证书有效期限未到的个人、单位、服务器、企业、组织、网站等提供网上服务和享受网上服务的各种实体，以及其他凡是广东 CA 各类证书的有效期限未到的证书持有者。

4.3.1.3 挂失流程

1) 用户可自行在广东 CA 的网站上进行挂失操作，也可到广东 CA 或其它业务受理点进行挂失申请。

2) 用户在广东 CA 的网站上进行挂失操作时要求用户输入证书业务受理号及密码，若在一天之内用户输入业务受理号或密码错误三次，则用户在当天内不能在网页上进行挂失操作。

3) 若用户在网页上输入信息正确并确认该证书的所有信息与自己的证书相同则可进行挂失操作。证书挂失后，在 OCSP 服务中显示的状态为"Unknown"。

4.3.1.4 取消挂失的流程

1) 挂失证书后，但还未到 RA 点报失，可以取消挂失数字证书。
2) 用户可自行在网页上进行取消挂失的操作，也可以到广东 CA 或其他业务受理点取消挂失。
3) 如果用户在网页上进行取消挂失的操作时，一天内连续输入错误的密码超过三次，则当天不能再在网页上取消挂失，用户可以到 RA 点进行取消挂失证书。

4.3.1.5 用户挂失的时间是无限制的（除非用户的证书有效期已到期，则用户的挂失操作无效）

4.3.2 证书废止

4.3.2.1 废止的原因

1) 用户没有指明
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广东 CA 进行的临时或永久性的证书废止措施。

4.3.2.2 废止流程

1) 用户报失
   i. 用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，到广东 CA 或其他业务受理点填写数字证书报失申请表格。
   ii. 业务受理员确认其证书持有者身份。
2) RA 废止证书
   iii. RA 管理员进入 RA 审批系统，输入报失证书的业务受理号。
   iv. RA 管理员及用户确认该报失证书。

v. RA 管理员完成相关证书废止操作。

3) CA 废止证书

vi. CA 管理员每天签发一次 CRL。

4.3.2.3 CRL 发布周期：1 个工作日

4.3.2.4 CRL 最大期限：7 天

4.3.2.5 当用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 www.cnca.net 上下载最新的 CRL。

第五章、 设备、管理和操作安全控制

5.1 物理安全控制

5.1.1 机房安全

广东 CA 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。

广东 CA 的数据主机房有四道物理保护层，用以监控和管理广东 CA 机房的物理通道。除主机房外，同时具有数据备份机房，切实保证广东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广东 CA 的规定要求执行。

广东 CA 机房属 A 类安全机房，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。只有经广东 CA 授权的人员才可以在广东 CA 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。

在广东 CA 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。广东 CA 的角色权限管理员负责设置和检查各业务 CA、CA 分中心和 RA 管理员的权限。各实体管理员的权限和相应的责任在其与广东 CA 签订的协议中有详细严格的规定。

5.1.2 电源和空调

5.1.2.1 广东 CA 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。

5.1.2.2 广东 CA 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。

5.1.2.3 广东 CA 对于电源和空调系统的要求，严格按照国家一级机房管理规定，并且定时对系统进行检查，确保其符合标准。

5.1.3 防水

广东 CA 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

广东 CA 装有自动感应的气体灭火、报警装置，同时与专业防洪部门协调，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

广东 CA 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

广东 CA 提供系统的热备份，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

广东 CA 提供数据的异地备份，该操作严格遵循广东 CA 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 角色分配及权限控制

5.2.1.1 CA 体系管理员

编号	角色名称	所需人数	角色分配及权限控制
1)	系统管理员	3	系统管理员，具有相关操作权限

编号	角色名称	所需人数	角色分配及权限控制
2)	高级 CA 管理员	2	具有管理 CA 管理员的权限
3)	CA 管理员	2	签发 CA 证书、TSA 证书、OCSP 服务器证书、管理员证书、VPN 证书、个人数字证书、单位数字证书、单位员工数字证书、服务器数字证书、Codesign 数字证书、SMIME 数字证书、CRL
4)	NS 管理员	2	命名空间管理员，负责整理 NS 树，创建 CA、VRA
5)	体系管理员	2	具有管理 CA 体系的管理员的权限
6)	系统审计员	2	负责审计 CA 证书、TSA 证书、OCSP 服务器证书、管理员证书、VPN 证书、个人数字证书、单位数字证书、单位员工数字证书、服务器数字证书、Codesign 数字证书、SMIME 数字证书的审计信息
7)	业务统计员	2	负责统计 CA 证书、TSA 证书、OCSP 服务器证书、管理员证书、VPN 证书、个人数字证书、单位数字证书、单位员工数字证书、服务器数字证书、Codesign 数字证书、SMIME 数字证书
8)	证书签发操作员	2	负责签发 CA 证书、TSA 证书、OCSP 服务器证书、管理员证书、VPN 证书、个人数字证书、单位数字证书、单位员工数字证书、服务器数字证书、Codesign 数字证书、SMIME 数字证书
9)	OCSP 管理员	1	
10)	TSA 管理员	1	
11)	邮件列表管理员	1	管理、修订
12)	角色权限管理员	2	为 RA 管理员设置和管理角色权限分配
13)	LDAP 管理员	2	
14)	数据归档管理员	2	负责数据归档

表格 6 CA 体系管理员角色表

5.2.1.2 RA 体系管理员

编号	角色名称	所需人数	角色分配及权限控制
1)	RA 身份审核员	由业务需求决定	个人数字证书、单位数字证书、单位员工数字证书、服务器数字证书、Codesign 数字证书、SMIME 数字证书
2)	RA 销售员	由业务需求决定	个人数字证书、单位数字证书、单位员工数字证书、服务器数字证书、Codesign 数字证书、SMIME 数字证书

表格 7 RA 体系管理员角色表

5.2.2 角色权限控制

广东 CA 系统的权限是为 CA 体系、每个 CA 和 RA 内置，不能被修改，而角色由权限组成，角色可以分配给管理员。CA 体系管理员只能对 CA 体系进行操作，而 RA 体系管理员只能对 RA 体系进行操作，两种类型的管理员的权限是分开的。

5.3 人事安全控制

5.3.1 人员资格要求

广东 CA 员工都经过严格的审查，合格方能录取。根据岗位职能需求，安排能胜任的可信任员工。员工的正式委任需经过上个月的考察期，关键岗位的考察期为六个月，根据考察结果安排相应的工作或做出相应的岗位调动，不合格者则剥离岗位或辞退。广东 CA 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。

广东 CA 对其关键的 CA 职员需进行严格的北京审查。RA 操作员的审查可以参照广东 CA 对可信任员工的考察方式。RA 也可在此基础上，增加考察和培训条款，但不得违背广东 CA 证书受理规程和广东 CA 的电子认证操作规范。

广东 CA 确立流程管理规则，据此员工受合同和章程的约束，不可泄漏广东 CA 证书服务体系的敏感信心。所有员工必须与广东 CA 签订保密协议，合同期满后仍然对企业重要的商业秘密承担保密义务，直至该秘密完全公开。同时 3 年内人不得从事与广东 CA 相类似的工作，报第三方公证。

5.3.2 背景审查

广东 CA 严格审查所有工作人员身份证明资料，同时还与有关政府部门和调查机构合作，完成对广东 CA 可信任员工的背景审查。

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

5.3.3.1 CA 培训

广东 CA 对所有员工进行以下内容的综合培训：

1) “企业人”的基本行为规范；
2) 电子商务基本知识及广东 CA 发展战略；
3) 电子商务法律热点介绍；
4) 广东 CA 安全原则和机制；
5) 系统及网络介绍；
6) 广东 CA 质量控制体系；
7) 岗位职责；
8) 广东 CA 的行政、保密等政策、标准和程序；
9) 电子商务技术；
10) 团队合作训练等。

同时还根据公司需要，每年选派优秀的员工接受国内外培训。

5.3.3.2 RA 培训

业务受理点及其下属营业点所有上岗人员应接受广东 CA 的培训，并经广东 CA 考核合格后，持证上岗。

业务受理点应接受广东 CA 的统一业务管理和业务考核。业务受理点向广东 CA 负责，其下属各营业点向业务受理点负责，严格执行广东 CA 的业务操作规范。由于营业点违规操作而导致的一切后果，均由业务受理点负责。

5.3.3.3 再培训

广东 CA 定期对员工进行再培训，以不断提高员工素质，使员工紧跟最新技术动向。同时根据广东 CA 策略调整、系统更新升级或功能增加等情况，广东 CA 也为员工进行继续培训，使其更快更好适应新的变化。

5.3.4 对未授权操作的处理

广东 CA 员工所有操作皆有记录，记录定期由专员审查。当发现员工涉嫌违规操作或已进行了未授权的操作，例如未经授权滥用权力或超出职权操作系统等，广东 CA 证实后将立即中止该员工进入广东 CA 证书认证体系。同时根据情节严重程度，对当事人做出相应处罚，包括内部处分、辞退等，情节严重者将送司法机关处理。当事人的证书和操作权限即时冻结或废止，同时所做的未授权操作将立即被废止失效，例如，废止未授权签发的证书等。

5.4 安全审计

5.4.1 审计周期

广东 CA 系统的安全审计周期为每周一次，如果出现特殊情况则另行作审计。

5.4.2 审计记录的保存

广东 CA 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。

5.4.3 审计记录的保存期限

广东 CA 系统的审计记录在数据库保存的期限为 2 年；离线保存的保存期限为 10 年。

5.4.4 审计记录的备份

广东 CA 保证所有的审计记录都按照广东 CA 的备份和程序进行备份。

5.4.5 审计采集系统

5.4.5.1 广东 CA 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) 广东 CA 网站

9) 时间戳服务系统

10) 网络安全防护系统

11) 其它广东 CA 认为有必要审计的系统

广东 CA 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。

5.4.6 审计结果的通知

广东 CA 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，将由广东 CA 决定。

5.5 存档

5.5.1 档案类型

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

5.5.2 档案的保存

广东 CA 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

广东 CA 系统档案的保存期限至少为 5 年。根据客户需求可增长期限。

5.5.4 档案备份

广东 CA 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

对于每一个广东 CA 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

广东 CA 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

广东 CA 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 广东 CA 遭攻击或发生事故时的灾难恢复

广东 CA 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，广东 CA 将按照灾难恢复计划进行系统的灾难恢复。具体由广东 CA 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

当广东 CA 的根私钥被泄漏时，广东 CA 将按广东 CA 的灾难恢复计划进行恢复广东 CA 根私钥。

5.7 CA 或 RA 业务终止

5.7.1 CA 业务终止

当广东 CA 打算终止业务情况下，广东 CA 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。

广东 CA 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，并按照相关法律规定的步骤操作，尽量减少对 CA 及证书持有人的影响。

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

业务受理点应建立业务档案，对用户资料严格保密，并按照广东 CA 的要求，以可靠的方式及时将用户资料交给广东 CA。业务受理点的代理业务终止之日起 10 个工作日内，业务受理点必须将所有用户资料无条件交给广东 CA。

第六章、 技术安全控制

6.1 密钥对的产生和安装

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、传送、安装等具备保密性、完整性和不可否认性。

6.1.1 密钥对的产生

6.1.1.1 广东 CA、各业务 CA 和 CA 分中心密钥对的产生

广东 CA、各业务 CA、CA 分中心、RA 皆具备签名密钥对，该密钥对是由国家密码委员会办公室（以下简称国密办）许可的加密设备生成的，由各实体控制管理。

证书持有人可使用广东 CA 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。证书持有人的密钥对的产生必须遵循国家法律和广东 CA 的 CPS。

广东 CA 支持多种模式产生的密钥对（详细参见具体的申请页面所列），证书申请人可根据具体需求进行选择。证书申请人的密钥对可以由申请人自行产生，也可以由 RA 代产生（此时密钥必须存储在国密办批准的不可导出的介质中，保证 RA 无法复制密钥对）。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。广东 CA 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

广东 CA 的私钥是在系统创建时自生产的，该私钥只能保存在系统中，禁止向外传递。

各业务 CA、CA 分中心和 RA 的密钥对由广东 CA 产生。各业务 CA 的私钥只能保存在系统中，禁止向外传递。各 CA 分中心和 RA 的私钥则由广东 CA 通过离线方式安全传送其私钥。

如证书申请人的密钥对是由 RA 代产生的，则 RA 将产生好的密钥对存入国密办批准介质中，封装好通过离线方式，发放给用户。

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。

6.1.4 CA 公钥的传递

广东 CA 的根公钥包含在广东 CA 自签的根证书中。各业务 CA 和 CA 分中心的公钥包含在由广东 CA 签发的 CA 证书链中。

各级业务 CA、CA 分中心证书签发后，组成多种完整的 CA 证书链，包括有个人证书 CA 证书链、单位证书 CA 证书链、服务器证书 CA 证书链、代码签名证书 CA 证书链和安全电子邮件证书 CA 证书链。广东 CA 支持从广东 CA 网站分别下载不同的 CA 证书链和一次性下载所有的 CA 证书链。

6.1.5 密钥长度

广东 CA 各实体的密钥对为不小于 1024 位的 RSA 密钥对。证书持有人的密钥对为 512 位或 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、广东 CA 认可的软、硬件产生。其中广东 CA 各实体的密钥皆由国密办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、广东 CA 认可的软件模块或硬件加密设备产生。

6.1.7 密钥用途

在广东 CA 证书服务体系中的密钥用途和证书类型紧密相关。

- 广东 CA 的签名密钥用于签发下级 CA、RA 证书和证书废止列表（CRL）；
- 各业务 CA 的签名密钥用于签发下级 CA 或用户证书；
- CA 分中心的签名密钥用于签发下级 CA 或用户证书；
- RA 的签名密钥用于确认 RA 所做的审批证书等操作；
- 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；
- 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，广东 CA 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，各业务 CA 证书有限期为 25 年，CA 分中心根据广东 CA 证书策略具体定制，但不能超过根证书期限。RA 和用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，但系统支持在根证书有效期内的任意期限，最短可定制到一天。

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

广东 CA 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

广东 CA 采用多人控制策略激活、使用、停止广东 CA 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。签名私钥从不进行托管，以保证其不可否认性。广东 CA 可以协助客户进行托管，但在技术上保证广东 CA 无法获取客户托管的私钥。

6.2.4 私钥备份

证书的持有者可以备份他们的私钥，但要确保这些私钥的安全。

密钥管理中心可以备份托管的私钥，并且要确保这些私钥的安全。备份托管的私钥的程序必须至少两人参与完成

6.2.5 私钥存档

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

在广东 CA 证书服务体系中，使用广东 CA 的软件可以把私钥导入密码模块中

私钥无法从硬件密码模块中导出。必须通过密码验证之后，才可能把私钥从软件密码模块中导出。

6.2.7 私钥在密码模块中的保存

证书的持有者可以将私钥保存在硬件密码模块中，也可以保存在软件密码模块中。

广东 CA 的签名私钥必须保存在硬件密码模块中。

6.2.8 激活私钥

在广东 CA 证书服务体系中，必须通过密码验证后，方可激活私钥。

6.2.9 停止私钥

在广东 CA 证书服务体系中，通过终止程序来停止私钥，并且把私钥从内存中清除。

6.2.10 销毁私钥

凡用户需要销毁私钥，应通知广东 CA，由密钥管理中心进行销毁。

6.3 敏感数据的保护

6.3.1 敏感数据的产生

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

6.3.2 敏感数据的保护

广东 CA 采取加解密机制等多种方式保护敏感数据，以避免为授权的使用。未授权用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

广东 CA 的 CA 系统的数据文件和设备由 CA 系统管理员维护，未经 CA 管理员授权，其它人员不能操作和控制 CA 系统；而其它普通用户也没有系统帐号和密码。广东 CA 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。广东 CA 系统密码有最小密码长度要求，而且必须符合复杂度要求，CA 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

广东 CA 的计算机系统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。广东 CA 使用的密码设备是通过国家密码委员会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

广东 CA 的软件设计和开发过程遵循以下原则：

- 第三方的验证和审核
- 安全风险和可靠性设计

6.5.2 安全性管理控制

广东 CA 的配置以及任何修改和升级都会记录在案并进行控制，并且广东 CA 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

广东 CA 有防火墙以及其他访问控制机制保护，其配置只允许已授权的机器访问。只有经过授权的广东 CA 员工才能够进入广东 CA 证书服务器、广东 CA 应用服务器、广东 CA 证书目录服务器、广东 CA 操作中心等设备或系统。所有授权用户必须有合法的电子密钥，并且通过密码验证。

6.7 数字时间戳

数字时间戳 (DTS: Digital Time Stamp) 是对时间信息的数字签名，主要用于实现确定在某一时间，某个文件确实存在和确定多个文件在时间上的逻辑关系功能。

广东 CA 提供精度为秒的时间戳服务。

第七章、 证书、CRL 及 OCSP

7.1 证书

证书支持现在主流的浏览器产品（包括 Microsoft IE 5.0 及后续版本、Netscape 4.0 及后续版本）和电子邮件客户端软件（包括 Microsoft Outlook 等）。可存放于计算机硬盘、智能卡、USB 电子密钥中。

7.1.1 个人证书

个人证书是广东 CA 专门为个人用户提供的证书，用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用户的其他信息。

7.1.2 单位/单位员工证书

颁发给独立的单位、组织，在互联网上证明该单位、组织的身份。单位数字证书根据各个单位的不同需要，可以分为单位证书和单位员工证书。单位证书对外代表整个单位，相当于单位公章；单位员工证书对外代表单位中具体的某一位员工。

7.1.3 服务器证书

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，其中包含了有关服务器以及服务器所属单位的信息。服务器数字证书可以使用户验证服务器的合法性，并创建客户端和服务器之间的安全连接。

服务器数字证书支持目前主流的 Web Server，包括但不限于：IIS、Lotus Domino、Apache、iPlant 等 Web 服务器。可存放于服务器硬盘或加密硬件设备上。

7.1.4 代码签名证书

为软件开发商提供对软件代码做数字签名的技术，可以有效防止软件代码被篡改，使用户免遭病毒与黑客程序的侵扰，同时可以保护软件开发商的版权利益。支持 Microsoft Authenticode Technology、Netscape Object Signing、Ms Office 2000/VBA Macro Signing 等代码签名技术。

7.1.5 安全电子邮件证书

结合使用数字证书和 S/MIME 技术对普通电子邮件做加密和数字签名处理，可以确保电子邮

件内容的安全性、机密性、发件人身份确认性和不可抵赖性。

7.2 CRL

证书一旦废止成功，该证书的序号将被列入证书的 CRL（证书废止列表）。CRL 是一种包含废止的证书列表的签名数据结构。CRL 的完整性和可靠性由它本身的数字签名来保证。用户可手动下载或在应用程序中设置自动查询来获取 CA 发布的最新 CRL。

广东 CA 提供为完整 CRL，增量 CRL 和分块 CRL 三种 CRL。它们之间各有所长，互为补充。

7.3 OCSP

由于 CA 签发的 CRL 需要一定的时间间隔，为了提高交易的安全性和可靠性，对交易安全性较高的应用系统应可以在线查询证书状态（OCSP）。广东 CA 提供证书状态在线查询服务，对于状态正常的数字证书，向查询方返回正常信息，对于状态非正常（包括挂失/废止等状态）的数字证书，返回证书无效信息。

第八章、 业务与法律说明

8.1 服务费用

8.1.1 广东 **CA** 数字证书的发放、验证和管理实行有偿服务，用户有义务按照规定向广东 **CA** 交纳相关服务费用。

8.1.2 广东 **CA** 数字证书一旦发放，广东 **CA** 不办理退证、退款手续。

8.2 保密

8.2.1 保密制度

8.2.1.1 广东 **CA** 制定并落实严格的信息保密规章制度，所有相关人员（包括广东 **CA** 及其业务代理机构的工作人员、证书持有者）必须遵守该规章制度，广东 **CA** 有权根据情况修改相关内容。

8.2.1.2 由广东 **CA** 制定及实施的信息保密规章制度符合国家保密机构的相关规定。

8.2.2 机密信息

8.2.2.1 与证书持有者证书公钥配对的私钥和密码是机密信息，证书持有者应当妥善保管，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，证书持有者应当自行负责承担一切责任。

8.2.2.2 证书持有者的个人/单位信息和商业信息、广东 **CA** 与业务代理机构间的商业信息等属机密信息，除非法律明确规定，一般不能在未经另一方许可的前提下擅自公开。

8.2.2.3 与广东 **CA** 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，除广东 **CA** 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。

8.2.2.4 除非法律明文规定，广东 **CA** 没有义务公布或透露证书持有者证书以外的信息。

8.2.3 非机密信息

8.2.3.1 由广东 **CA** 网站或手册公布的信息：证书持有者的数字证书、证书废止情况、证书申请流程、证书使用指南等信息，此类信息仅供用户下载使用，不得转载或用于任何商业用途，广东 **CA** 保留追究责任的权利。

8.2.3.2 向法律执行机关披露的信息：当广东 **CA** 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操作规范中具有机密性质的信息时，广东 **CA** 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，广东 **CA** 无须承担任何责任。

8.2.3.3 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，要求广东 **CA** 公开或披露他所拥有的机密信息，广东 **CA** 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，广东 **CA** 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。

8.2.4 保密要求

8.2.4.1 广东 **CA** 执行严格的信息保密规章制度以确保只有经广东 **CA** 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。

8.2.4.2 除非符合本认证操作规范的规定，否则广东 **CA** 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。但广东 **CA** 的证书资料库中应包含证书、废止及其它证书状况资料。

8.2.4.3 广东 **CA** 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)**广东 **CA** 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。广东 **CA** 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。

8.2.4.4 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。

8.3 知识产权

8.3.1 广东 **CA** 享有并保留对证书以及广东 **CA** 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。

8.3.2 “网证通”电子认证系统是由广东 **CA** 设计、开发和运行的，因此广东 **CA** 拥有该软件系统的知识产权。

8.3.3 所有由广东 **CA** 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广东 **CA** 的知识产权范围。

8.3.4 在没有广东 **CA** 预先书面同意的情况下，证书持有者不能在任何证书到期、废止、或终止的期间或之后，使用或接受任何广东 **CA** 使用的名称、商标、交易形式或可能与之相混淆的名称、商标、交易形式或商务称号。

8.3.5 证书申请人（于接受申请时即为用户）声明并保证其交付（给广东 **CA**）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（于接受申请时即为用户）应为广东 **CA** 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。

8.4 权利与义务

8.4.1 CA 的权利与义务

8.4.1.1 广东 **CA** 享有的权利主要有以下方面：

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，广东 CA 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；对单位数字证书申请者，除对具体的经办人要求提供上述个人资料外，还要求提供申请单位资料——如单位名称、单位地址、单位组织机构代码、单位电子邮箱、电话、传真、单位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、所属单位名称、所属单位地址等资料，还同时要求提供申请单位和经办人的有关资料及其相关有效证件的原件和复印件。广东 CA 或广东 CA 授权的受理审核单位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，有权委托相关法人单位作为业务受理审批单位（即业务受理点）从事数字证书的受理、数字证书用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用户的不同需要。

④收取费用的权利：广东 CA 有权向证书申请者收取费用。

⑤广东 CA 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广东 CA 对于下列情况之一，将有权主动废止所签发给证书持有者的证书：

- 证书申请初始注册时，提供不真实材料；
- 违反国家法律或者其它规章制度，不应签发证书的；
- 有盗用、冒用、伪造或者篡改他人证书的；
- 不履行广东 CA 的内部规范，如《认证业务操作规范》中的规定；
- 与证书中的公钥相对应的私钥被泄密；
- 证书中的相关信息有所变更；
- 由于证书不再需要用于原来的用途而要求终止；
- 证书的更新费用未收到；
- 其他情况。

⑦广东 CA 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；除未经证实的证书用户资料外，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。

⑧当使用或信赖证书的证书信赖者或广东 CA 的业务代理机构和雇员的违约行为或其他行为导致广东 CA 发生任何损失、损坏或债务责任和法律费用以及成本损耗，广东 CA 有权要求赔偿。

8.4.1.2 广东 CA 义务

广东 CA 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，法律规范的广东 CA 所履行的义务包括：

①广东 CA 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，即所发放认证证书中的公共密钥同某个确定身份的人是一一对应的，这就要求广东 CA 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，广东 CA 还享有撤消认证证书效力的权利。

②广东 CA 有保密的义务，除其他法律另有规定外，广东 CA 不得对外披露以下信息：一是数字证书申请人向广东 CA 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；二是用户委托广东 CA 保管的私钥。在任何数字证书被废止后的五年内，广东 CA 应当保存该数字证书的相关信息。

③广东 CA 有告知的义务，广东 CA 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。

概括起来，广东 CA 应当向社会公开披露以下内容并保证该内容的准确完整：一是根证书；二是数字证书上所列明的数字信息；三是用户的公钥；四是认证业务操作规范（CPS）；五是废止名单（CRL）；六是其他任何影响数字证书安全性能或者广东 CA 服务能力的事实。

④广东 CA 应履行的义务还包括：在广东 CA 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，接受证书用户的更新证书或废止证书等的要求；如获悉任何对用户证书的有效性与可信度具重大影响的事实，应立即通知证书用户。

8.4.2 RA 的权利与义务

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

8.4.3 证书持有者的权利与义务

8.4.3.1 证书持有者的权利

证书持有者应享有以下权利：

①获得有效合格的数字证书的权利：证书持有者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提出中止或废止数字证书的权利：在前述的有关广东 CA 应中止或废止数字证书的条件下，证书持有者或其代理人有权提出中止或废止证书的申请。

8.4.3.2 证书持有者的义务

在电子认证关系中，证书持有者（或证书用户）是广东 CA 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）：

证书持有者对证书内容真实性的保证：证书持有者一旦接受了广东 CA 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。

证书持有者对广东 CA 做出的所有重大陈述，包括证书持有者已知的所有信息和在证书中的表述．无论是否经过广东 CA 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：真实陈述广东 CA 颁发证书时要求其提供的事项，是证书用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：

证书持有者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，“广东 CA 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证书持有者的私人密钥的保护程度，广东 CA 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，保证证书持有者的私人密钥的安全。

当证书颁发并接收之后，证书持有者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。它是证书持有者所应负的针对不特定的任何人的义务。实际上，它是一种与广东 CA 的公正发布信息的义务相并列的社会责任。没有证书持有者对其私密钥的独占性控制，广东 CA 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，不仅是证书用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。证书持有者若违反了该义务，将承担相应的法律责任。

③通知的义务：

如果证书持有者的私密钥出现问题，例如遗失、盗用、破坏或者泄密等，一旦证书持有者私钥失密，就会出现他人冒证书持有者之名进行交易的危险，因此，此时证书持有者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，包括广东 CA；同时向广东 CA 申请中止或废止该证书。

④使用可信赖系统之义务：证书持有者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：证书持有者应向广东 CA 交纳服务费用，主要在接受证书时交纳，在中止或废止证书时，证书持有者向广东 CA 也要交纳费用。

8.4.4 证书信赖者的权利与义务

所有的证书信赖者在信赖任何证书的时候，须要遵守以下几点义务：

- 证书信赖者须熟悉电子认证业务操作规范以及和证书持有者证书相关的证书政策，还须了解和遵守证书的使用目的。证书信赖者必须确保证书的确用于预定的目的。
- 证书信赖者在信赖证书持有者的证书前，必须根据相应的最新的证书废止列表（即黑名单 CRL）检查证书的状态，查明证书是否还在有效期内。
- 当证书信赖者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”，证书信赖者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、未经废止的或更新的证书，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。必要时有权向广东 CA 联系和查询。

8.5 法律免责事由

免责事由又称为免责条件，是指当事人即使违约也不承担责任的情形。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。免责条件主要有：

8.5.1 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，广东 CA 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（如证书持有者）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证书用户的“责任书”中，也可被规定在广东 CA 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广东 CA 的操作失败或迟延的，广东 CA 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。

8.5.2 免责条款

广东 CA 不对由于意外或其他不可抗力造成的操作失败或延迟承担任何损失、损坏或赔偿责任。

广东 CA 一般在提供给证书持有者的“数字证书责任书”中，都有事先告知证书持有者的免责条款规定：广东 CA 发放的各类型数字证书只能用于在网络上标识身份、加密数据、保证网络安全通讯等相应证书规定的用途，不能作为其他任何用途。若证书持有者将其数字证书用于其他

用途，广东 CA 不承担任何责任。

广东 CA 在进行身份认证或证书持有者下载数字证书时，将充分遵守广东 CA 的安全操作流程。如果由于非广东 CA 自身的原因而造成的广东 CA 设备故障、线路中断，导致签发数字证书错误、延迟、中断或者无法签发，广东 CA 不负任何赔偿责任。

广东 CA 在签发数字证书之前，事先就与证书申请者签定电子认证服务协议，明确规定广东 CA 不承担任何形式的担保和义务，具体条款包括以下：任何销路担保；保证一定适用于特定目标的担保；以及提供的任何相关信息的精确性的承诺，和所有由于缺乏妥善管理和疏忽引起的责任。其他未例举的担保责任；如果证书申请者故意或无意地提供不完整、不可靠或已过期的信息，而他又根据正常的流程提供了必须的审核文件，由此得到了广东 CA 签发的数字证书。由此引起的经济纠纷由证书申请者全部承担，广东 CA 不承担与证书内容相关的法律和经济责任，但可以根据受害者的请求提供协查帮助。广东 CA 也不承担任何其他未经授权的人或组织以广东 CA 名义编撰、发表或散布不可信赖的信息所引起的法律责任。广东 CA 仅仅提供电子沟通或交易中签名的“不可抵赖”的依据，但并不对此承担法律责任等等方面的约定。

8.6 理赔

8.6.1 在广东 CA 违反了前文 8.4.1 款条例规定的职责，广东 CA 承担赔偿责任（法律免责除外）。赔偿限制如下：

广东 CA 所有的赔偿义务不得高于这种证书适用的债务上限，这种上限可以由广东 CA 改动。

广东 CA 只有在广东 CA 证书有效期限内承担这种损失或损害赔偿。

8.7 CPS 的有效期与终止

广东 CA 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 请访问广东 CA 网站以获得，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。

8.8 修订

8.8.1 广东 **CA** 有权在合适的时间修订、修改和改变本认证操作规范书中任何术语、条件和条款，而且无须预先通知任何一方。

8.8.2 广东 **CA** 有权在广东 **CA** 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。

8.8.3 所有的修正、修改和变化在公布后立刻生效。证书持有者如不在修改结果后公布的限定天数内废止证书，就视为同意这种修正、修改和变化。所有以书面形式提供给证书持有者的内容，按以下规则发送：

a) 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；

b) 接受者是个人则向其申请书上规定的地址发送；

c) 这些通知可能用快递或挂号信的方式发送。广东 CA 有权选择通过电子邮件（e-mail）向证书持有者发送通知，邮件地址在证书持有者申请证书时已注明了。

8.8.4 所有发送给广东 **CA** 的通知应以书面形式传递。所有这些通知应采用快递或挂号信的方式发送。任何发送给广东 **CA** 的通知可以通过电子邮件（**e-mail**）传递，但这种通知只有在广东 **CA** 收到证书持有者的 **e-mail** 通知后 **24** 小时内，收到证书持有者书面材料，方为有效。

8.9 其他规定

8.9.1 各种规范的冲突

若本认证操作规范的规定与其它规定、指导方针或协议相互抵触，用户必须接受本认证操作规范的约束，除非本认证操作规范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

签署日期在本认证操作规范首次公开发行之前，或 (ii) 该协议明确地优于本认证操作规范，因此必须由该协议规范所有当事人。

8.9.2 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**：证书为广东 CA 的产权所有。本规范旨在保护用户的隐私，避免未经授权者公布其证书。
- **认证操作规范**：本认证操作规范的产权为广东 CA 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用户（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，公开密钥为用户（或其雇主或委托人）所有。

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

8.9.3 损害性资料

证书申请人与用户不能把包含以下言论的任何资料提交给广东 CA 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。

8.10 争议解决

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。

8.11 有关法规

8.11.1 监管法律

本认证操作规范在各方面服从国家法律的管制和解释。

8.11.2 其它

若要出口使用于广东 CA 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。

第九章、 定义和缩写

1. CNCA

广东省电子商务认证中心（有限公司）的英文简称。

2. CPS（Certification Practice Statement）

认证操作规范的英文简称。明确规定广东 CA 在审批、签发、发布和废止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。

3. 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 为电子商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、废止等一系列管理。

4. 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。

5. 认证（Certification）

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。

6. 数字签名（Digital Signature）

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。

7. 私人密钥（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。

8. 公开密钥（Public Key）

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。

9. 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，用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，如果要一个用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用户的身份。

10. 数字证书

数字证书又称为数字标识 (Digital Certificate ，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单位在 Internet 上的身份证。

11. 试用型数字证书

试用型数字证书种类有个人数字证书、服务器数字证书和代码签名数字证书，使用范围与正式数字证书一致，主要供用户测试使用，方便用户认识数字证书、了解数字证书、懂得如何使用数字证书。同时数字证书有效期仅为一个较短的时间。

12. CRL （Certificate Revocation List）

数字证书废止列表的英文简称。CRL 中记录所有在原定失效日期到达之前被废止的数字证书的用户数字证书序列号，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、下次废止列表的预定发行日期、遭更新或废止的数字证书序号，并说明遭更新或废止的时间与理由。声明了主体的名字或签发中心的身份，确定签名者的身份，包括签名者的公开密钥，表明了数字证书的操作时限，还包括数字证书的序列号。

13. 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废止列表（CRL）。

14. 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。

15. DTS (Digital Time Stamp)

即数字时间戳服务，向用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。

16. FTP　File Transfer Protocol　文件传输协议

17. GMT　Greenwich Mean Time　格林威治标准时间

18. HTTP　Hypertext Transfer Protocol　超文本传输协议

19. HTTPS　Hypertext Transfer Protocol with SSL　采用 SSL 的超文本传输协议

20. PIN　Personal Identification Number　个人识别号

21. PKCS　Public Key Cryptography　公开密钥密码法

22. PKI　Public Key Infrastructure　公开密钥基础架构

广东省电子商务认证中心

Guangdong Electronic Certification Authority

网证通 NET CA

地址：广州市中山大道华景路一号南方通信大厦九楼
Add：Floor9. Southern Communication Plaza No.1
Huajing Road. Zhongshan Av.Guangzhou China
邮编(Zip)：510630　　**网址**：www.cnca.net
电话(Tel)：+8620-38638302 / 38638303
传真(Fax)：+8620-38638308
E-Mail:sales@cnca.net