深圳 CA 证书策略

（CP）

版本 V1.0

2019 年 06 月

https://www.szca.com

目　录

版本信息

档名	深圳 CA 证书策略（CP）		保密级别	公开
本文件历史变更记录				
版本	生效时间	作者	发布者	说明
V1.0	2019.06.25	证书策略发展小组	安全策略管理委员会	

版权声明

第一章 简介

1.1 概述

深圳市电子商务安全证书管理有限公司,简称深圳 CA 中心、深圳 CA，或 SZCA（以下统一简称“SZCA”），成立于 2000 年 8 月，是依法设立的合法权威的第三方电子认证服务机构。SZCA 依照《中华人民共和国电子签名法》、《电子认证服务管理办法》等法律法规，及工业与信息化部、国家密码管理部门等的要求，向公众（包括政府机构、企事业单位及个人）提供身份认证和信任服务。

证书策略（CP，Certificate Policy）是一套有关证书安全要求的规则集，阐述证书对具有共同安全需求的某一特定群体、团体，或某类应用的适用范围和使用要求的规则。本证书策略的适用范围为 SZCA 在中国境内发放的非跨境互认类证书。

1.2 文档名称与标识

本文档的名称为《SZCA 证书策略（CP）》。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构(Certificate Authority)

电子认证服务机构（Certification Authority，简称 CA）作为可信任的第三方，对个人、实体及设备进行主题信息及其他属性与公钥绑定的确认，颁发数字证书，并提供证书验证服务。CA 承担证书签发、更新、吊销，密钥管理，证书查询，证书黑名单（又称证书吊销列表或 CRL）发布，证书策略以及业务规则的制定等工作。SZCA 及其下属子 CA 共同构成电子认证服务机构。

1.3.2 注册机构（Registration Authority）

注册机构（Registration Authority，简称 RA）代表 CA 建立和执行注册过程，审查确认证书申请者的身份，批准或拒绝证书申请者。根据职能分配，可能负责受理申请、审核资料、识别鉴定申请人身份、决定批准或拒绝证书申请等职责。

成为 SZCA 的 RA，须与 SZCA 签订相关的授权或者合作协议，获得授权并按 SZCA 要求进行运营。

1.3.3 订户（Subscriber）

订户，即证书持有人，是指从 SZCA 接受证书的实体。在电子签名应用中，订户即电子签名人。

1.3.4 依赖方（Relying Party）

证书依赖方是指在 SZCA 证书服务体系之内依赖于数字证书及其验证的电子签名真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是订户，但不仅限于订户。

1.3.6 其他参与者（Other Participants）

为以上未提及的隶属于 SZCA 证书体系的其它实体，例如 SZCA 选定的第三方的身份鉴别机构、目录服务提供者等与 PKI 服务相关的参与者等等。

1.4 证书应用

1.4.1 适合的证书应用

SZCA 的证书可以用于网络身份认证、网络安全登录、信息传输保护、通信密钥协商、电子文件签署，还可进行客户端访问权限控制等。根据证书级别及使用人的要求，在不违反法律法规，及电子认证相关规则、电子认证服务协议的规定情况下，可选择其他适合的证书用途。

1.4.2 限制的证书应用

SZCA签发的证书禁止的应用范围包括：

1. 《中华人民共和国电子签名法》第三条规定的情形；
2. SZCA与订户约定的证书禁止应用范围；
3. 证书禁止在任何违反国家法律法规的应用系统领域中使用。

1.5 策略管理

1.5.1 策略文档管理机构

SZCA 的证书策略管理机构为 SZCA 安全策略管理委员会，当需要修订 CP 时，由安全策略管理委员会牵头组织技术中心、运营中心、项目管理部、财务部、人事部等的管理人员，核心技术人员组成的“SZCA 证书策略发展小组”，并最终由 SZCA 安全策略管理委员会审核并发布。

1.5.2 联系人

如对本 CP 有任何疑问，请联系 SZCA 安全策略管理委员会：

电话：0755-26588399

电子邮件：cps@szca.com

邮寄地址：深圳市南山区高新中二路深圳软件园 8 栋 301 室

邮编：518057

1.5.3 证书策略审批机构

“SZCA 安全策略管理委员会”是决定 SZCA 电子认证服务所有策略符合性的最高决策机构。由 SZCA 高级管理人员、核心技术人员和法律顾问组成，负责决定本 CP 及其他补充或附属于本 CP 的文件的符合性及修订、升版的核准与驳回。

1.5.4 证书策略审批流程

SZCA 的 CP 由“SZCA 证书策略发展小组”起草拟定后，提交 SZCA 安全策略管理委员会审核。如果因为标准的变化、技术提高、安全机制的增强、运营环境的变化和法律法规的要求等对 CP 进行修改，由“SZCA 证书策略发展小组”提交修改建议报告，提交 SZCA 安全策略管理委员会批准，批准通过后方可对外发布。

1.5.5 CP 发布

在 CP 修改审批通过后，由 SZCA 安全策略管理委员会在 SZCA 网站 https://www.szca.com 上发布。自发布之日起，各种形式提供的 CP 必须与网站上 CP 保持一致，“SZCA 安全策略管理委员会”负责依法在 CP 公布之日起三十日内向工业与信息化部备案。

1.6 定义和缩写

表 1.1-定义与缩写

缩写/名词	定义
SZCA	深圳市电子商务安全证书管理有限公司的缩写
电子认证服务机构	(Certificate Authority, CA)SZCA 及子 CA 统称为电子认证服务机构
注册机构	CA 注册机构简称 RA。与 SZCA 签署注册机构协议，被 SZCA 授权发行 SZCA 证书的代理机构。注册机构负责处理证书申请者提出的证书申请信息，并提交 CA
发证机构	包含 SZCA 授权的注册机构、注册分支机构、受理点证书发放机构。发证机构为证书申请者发放 SZCA 证书。
SZCA 安全策略管理委员会	由 SZCA 任命的负责 SZCA 安全策略核准及执行的组织
SZCA 超级管理员	负责实施 CA 政策、增加新 CA 管理员、验证审计记录、电子认证业务规则的执行情况承诺
SZCA 系统管理员	负责安装、配置和维护 CA 系统的软硬件系统，负责 CA 服务器的启动和中止
SZCA 录入员	负责录入证书申请者提交的信息
SZCA 审核员	负责审核证书申请信息
SZCA 审计员	CA 审计员（Auditor）负责 CA 系统的证书统计，系统审计
SZCA 证书制作员	负责为证书申请者制作证书
SZCA 数字证书签发系统	为 SZCA 证书申请者签发、管理数字证书的软件系统
SZCA 白皮书	SZCA 白皮书是 SZCA 的一个支持 SZCA 数字证书相应政策的详细的操作

	规则和操作步骤
注册机构协议	一份合同，它详细地概括了 SZCA 指定的注册机构的程序、责任和义务
注册分支机构协议	一份合同，它详细地概括了 SZCA 指定的注册分支机构的程序、责任和义务
依赖方	（Relying Party）指基于对数字证书或电子签名的信任而从事有关活动的人
订户	个人、集体、单位、组织、或者其它拥有任何 SZCA 证书的人或实体
证书口令授权码	证书口令指证书中私有密钥的保护口令 SZCA 为证书申请者颁发证书时生成的字符组合。与参考码相对应
证书序列号证书口令	唯一标识证书的字符证书口令指证书中私有密钥的保护口令
甄别名证书序列号	甄别名（Distinguished Name）简称 DN，包含用户的属性信息唯一标识证书的字符
密钥管理中心甄别名	密钥管理中心简称 KMC，负责密钥的产生、存储、归档等工作甄别名（Distinguished Name）简称 DN，包含用户的属性信息
电子签名密钥管理中心	电子签名，是利用公开密钥算法等方法保证信息传输过程中信息的完整和提供信息发送者的身份认证及不可抵赖性的一种技术密钥管理中心简称 KMC，负责密钥的产生、存储、归档等工作
私有密钥/电子签名	私有密钥指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。 私钥是经由数字运算产生的密钥，用于制作电子签名的数据，亦可依据其运算方式，就相对应的公开密钥加密的文件或信息予以解密。 电子签名，是利用公开密钥算法等方法保证信息传输过程中信息的完整和提供信息发送者的身份认证及不可抵赖性的一种技术
公开密钥/私有密钥	公钥是经由数字运算产生的密钥，用于解密电子签名，确认电子签名人的身份及电子签名的真实性。 公钥可以公开，一般标示于在线数据库，存储库或其他公共目录中，使任何希望得到公钥的人都能得到。 电子签名验证数据是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。如果电子签名制作数据表现为私钥，则电子签名验证数据就是公钥指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。 私钥是经由数字运算产生的密钥，用于制作电子签名的数据，亦可依据其运算方式，就相对应的公开密钥加密的文件或信息予以解密
签名密钥对	证书申请者申请证书时由用户端产生。主要用于用户的签名和验证。包含一对私有密钥和公开密钥公钥是经由数字运算产生的密钥，用于解密电子签名，确认电子签名人的身份及电子签名的真实性。
加密密钥对	证书申请者申请证书时由 KMC 产生。主要用于用户信息的加解密。包含一对私有密钥和公开密钥证书申请者申请证书时由用户端产生。主要用于用户的签名和验证。包含一对私有密钥和公开密钥
CRL	CRL（Certificate Rovocation List），即数字证书吊销列表的英文简称。CRL 中记录所有在原定失效日期到达之前被吊销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 CA 机构的

	名称、发行日期、下次吊销列表的预定发行日期、变更或吊销的数字证书序号，并说明变更或吊销的时间与理由。
CPS/CP	Certification Practice Statement 认证业务规则 Certificate Policy 证书策略
DES	Data Encryption Standard 数据加密标准
LDAP	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吊销列表（CRL）
OCSP	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
PKCS	PKCS （Public Key Cryptography Standard），公开密钥密码算法标准
PKI	PKI（Public Key Infrastructure），公开密钥基础设施
RFC	征求意见稿（Request For Comments，缩写为 RFC），是由互联网工程任务组（IETF）发布的一系列备忘录。请求评注标准。
RSA	Rivest-Shamir-Adleman RSA 算法
SSL	Secure Sockets Layer 安全套接字层
PIN	Personal Identification Number 个人识别码

第二章 发布和信息库责任

2.1 信息库

SZCA 信息库是一个对外公开的信息库，包括但不限于以下内容：证书策略（CP）、电子认证业务规则（CPS）、相关协议、证书、证书吊销列表（CRL）、证书在线状态查询（OCSP）、技术支持手册、SZCA 网站信息以及 SZCA 不定期发布的信息。

2.2 认证信息发布

SZCA 需要发布的信息包括证书策略、电子认证业务规则、证书使用和服务相关的协议、证书、证书吊销列表、证书在线状态查询等。

SZCA 提供明确的访问位置和方法，通过在线的方式对外发布证书、证书吊销列表和证书在线状态查询。SZCA 信息发布官方网址为:https://www.szca.com.。

2.3 发布时间或频率

SZCA 最新修订的 CP 及 CPS 一般于批准后的 5 个工作日内发布到信息库网站 https://www.szca.com 上。

CRL 在 24 小时内自动更新，特殊紧急情况下也可通过人工手动方式变更 CRL 列表。

SZCA 一旦由于某些原因需要发布与其相关的公告、通知以及其他相关公众信息。SZCA 将在最快时间内在其网站 https://www.szca.com 上进行发布。

2.4 信息库访问控制

SZCA 不对包括 CP、CPS、证书、证书状态信息和 CRL 的访问进行限制，但 SZCA 保留设置访问浏览控制机制的权利。

SZCA 设置信息访问控制和安全审计措施，保证仅授权人员可对信息库中的相关信息进行编辑、增加、删除、修改等操作。

第三章 识别与鉴别

3.1 命名

3.1.1 名称类型

SZCA 签发的数字证书符合 X.509 标准，分配给证书持有者的主体甄别名（Distinguished nam），采用 X.500 命名方式，根据实体的类型不同，实体名称可以是姓名、组织机构名、部门名、商标名、电子邮件地址、域名或 IP 地址等。

3.1.2 对名称意义化的要求

标志名称所采用的用户识别信息，必须具有明确的、可追溯的、肯定的代表意义，不允许匿名或者伪名等出现。

3.1.3 订户的匿名或伪名

SZCA 不接受或者允许任何匿名或者伪名，仅接受可追溯的名称作为唯一标识符。使用伪名或伪造材料者申请的证书无效，一经证实立即予以吊销。

3.1.4 不同命名的解释规则

DN 内容一般由 CN、OU、O、C 四部分组成，其中 CN 用来表示用户名，OU 用来表示用户所属部门，O 用来表示用户所属组织机构名称，C 用来表示用户所属国家。

3.1.5 名称的唯一性

认证机构的所有证书持有者，证书主体甄别名在 CA 信任域内是唯一的。如出现不同实体重名或同一主体多张证书，通过顺序号或证书主题区分证书。

3.1.6 商标的识别、鉴别和角色

认证申请人不得在其认证申请中使用会侵犯他人知识产权或商标专用权的名称。然而，SZCA 不会核查在认证申请中所出现的名称的认证申请人是否拥有该知识产权或商标专用权，亦不会仲裁、调解、或解决有关任何因网域名称、商标名称、服务标章所有权所引起的争议，当此类争议出现时，SZCA 将依照先申请先使用的原则，并有权在认为有必要时驳回或挂起相关证书申请直到争议解决，且不需对任何证书申请人负法律责任。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

SZCA 通过证书申请信息中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 CA 证书服务体系中，私钥在客户端生成，证书申请信息中包含用私钥进行的数字签名，CA 用其对应的公钥来验证这个签名。

CA 机构要求证书申请人必须保管好自己的私钥。证书申请人被认为是私钥的唯一持有人。

3.2.2 组织机构身份的鉴别

组织机构须由法定代表人本人申请，或委托授权代理人，负责证书申请相关事宜，包括提交证书申请资料，签署订户服务协议，表示接受 CP/CPS/服务协议的条款内容，并愿意承担相关的法律责任。

在为组织机构或其员工、设备签发证书时，SZCA 应对组织机构的身份作以下审查鉴别：

1) 确认组织机构是真实存在的、合法的实体

确认方式是依靠政府、上级、主管机构发放的组织机构身份证件（例如组织机构代码证、工商营业执照）、由具有公信力的政府机关出具的文件、权威第三方提供的身份证明、利用第三方数据库服务，证明该机构确实存在。

2) 确认该组织机构知晓并授权证书申请

由组织机构盖章确认的申请文件、由组织机构盖章确认的组织机构身份证明文件或核查原件、通过验证法人手机号向其发送含有随机短信数字、使用对公账号打款等方式，确认该组织机构知晓。依靠经组织机构签名盖章的书面授权委托书，确认代表机构进行证书申请的个人是否得到足够的授权。利用数据库服务，确认组织机构申请资料的真实性。

3) 验证申请代理人的身份

要求申请人本人提交法定的身份证明文件。利用数据库服务或设备，确认身份证明文件的真实性。

4) 验证机构个人身份（仅在机构个人证书情形下适用）

当在申请机构内部个人证书时，除机构身份证件、申请人身份证件外，还需提供证书主体个人的相关身份信息，一般是提供身份证，但也可由其所属的组织机构出具身份证明材料（须加盖机构公章），据以核实个人身份的真实性。

5）若以上信息及验证无法达到鉴别要求的，SZCA 可要求申请者额外提供其他身份证明材料，并采取适当合理的鉴别手段审查上述证明材料。

3.2.3 个人身份的鉴别

自然人申请数字证书，应提交合法有效的个人身份证件或个人身份信息，并与 SZCA 签订订户协议等服务协议，愿意承担相关的法律责任。订户申请 SZCA 的数字证书前，应

了解所申请证书对应的 CP 和 CPS 的规定。

个人的有效身份证件包括但不限于：居民身份证、户口簿、护照、外国人居民永久身份证、台湾居民来往大陆通信证、港澳居民来往内地通行证、军官证、警官证、士兵证、士官证、文职干部证等。根据证书的安全等级及鉴别强度，SZCA 可能需要订户进行生物特征识别，补充提交手机号、金融账户等信息进行多因子验证，申请人应予以配合。

3.2.4 电子邮箱的鉴别

对电子邮箱的鉴别，只会验证电子邮箱是否属于用户使用，并不会验证邮箱是否由用户用实名注册。电子邮箱鉴别程序如下：

1. 申请人提交以下身份证明文件，并填写完整申请表：
   - 订户身份证件；
   - 法定代表人身份证件，或授权代理人身份证件；
   - 授权委托书（如为代理人办理）。

   身份证件均校验原件，留存复印件
2. SZCA 将发送验证邮件至订户提交的电子邮箱中，订户将收到的验证内容，提交至 SZCA，如一致则验证通过。

3.2.5 设备身份的鉴别

针对设备证书，SZCA 将鉴别设备及其权属人、控制人即订户的身份信息，具体鉴别内容如下：

- 确认订户、申请人、授权申请等的真实性

  订户为机构的，申请材料提交参照 CP3.2.2 执行，即提交设备所有权人——机构订户的身份证明文件、法定代表人身份证件、或授权代理人身份证件及授权委托书（身份证件均交验原件，留存复制件）；

  身份鉴别参照 3.2.2-3.2.3 执行。
- 确认设备合格性、权属

  申请人提交设备的产权证明文件与合格证（均交验原件，留存复印件）；

  对设备身份、资质或相关属性的鉴别，可采用现场调查、勘验方式，实地验证设备的序列号等相关信息。

3.2.5 不需验证的订户信息

无规定。

3.2.6 授权、权限的确认

当法人等组织机构通过授权第三人代理申请某一类型证书时，SZCA 和其授权的证书服务机构还需要审核被授权人的身份和资格，包括被授权人的身份资料和授权证明，并且有权通过电话、信函或其它方式与授权人进行核实确认，以审核该授权行为的合法性，或利用第三方数据库资源验证被授权人身份。

3.2.7 互操作准则

无规定。

3.3 密钥更新请求的识别与鉴别

一般情况下，证书的有效期为一年。SZCA 有权根据具体情况决定证书有效期长短。 在证书有效期届满前申请证书更新的，证书更新的同时会产生新的密钥对；当证书中用户的相关信息发生变化或怀疑密钥有安全性问题，SZCA 将会签发新证书，产生新的密钥对。

3.3.1 常规的密钥更新的识别与鉴别

SZCA 需要订户提供书面申请进行密钥更新操作，密钥更新的同时证书也进行更新，订户更新密钥的流程，详见本 CP4.7 证书密钥更新。

3.3.2 吊销之后的密钥更新的识别与鉴别

证书吊销后的密钥更新，等同于订户重新申请证书，其要求与初次申请时的识别与鉴别方式相同。

3.4 吊销请求的识别与鉴别

由证书订户本人或授权人申请吊销时，SZCA 或授权的注册机构应当审核吊销申请者的书面申请材料和证书 DN 信息，同时需要重新进行身份识别与鉴别，身份验证流程与初始申请证书时相同，详见 CP3.2.2 组织机构身份的鉴别和 CP3.2.3 个人身份的鉴别，在审核通过的情况下由 SZCA 或授权注册机构进行吊销操作。

如果是因为订户没有遵守 SZCA CPS 或其它协议、法律及法规所规定的责任和义务，或出现本 CP4.9.1 中描述的其它情形，SZCA 或授权注册机构主动吊销订户证书时，无须对订户身份进行识别与鉴别。

第四章 生命周期操作要求

4.1 证书申请

4.1.1 证书类型

目前，SZCA 提供正式证书和测试证书两种类型。测试证书是 SZCA 提供给用户仅为测试使用的证书，SZCA 不承担任何证书真实性的责任。SZCA 对正式证书依法承担本 CP 规定的义务和责任。

根据订户或证书主体类型，正式证书可以分为个人证书、机构证书、邮件证书和设备证书。

4.1.1 证书申请实体

任何自然人、具有独立法人资格的企事业单位、社会团体等各类组织机构需要在应用中进行基于数字证书的身份鉴别、需要采用数字签名及实现信息加密时，可向 SZCA 及其授权机构提出证书申请。

个人证书由使用者本人提出申请；企业证书由企业等组织机构之被授权人提出申请；设备证书由设备所有权人之被授权人提出申请。

4.1.2 注册过程与责任

1. 注册过程

目前，SZCA 的证书申请方式有线下申请与在线申请两种方式。申请人使用不同渠道办理证书时，均需首先根据所申请证书的类型，依照各项目“办理指南”将申请表格填写完整，并将所需申请资料准备齐全，递交 SZCA 或 SZCA 授权注册机构。

根据相关法律法规，申请者必须真实填写证书申请信息，并遵守《深圳市电子商务安全证书管理有限公司电子认证服务协议》，否则 SZCA 有权拒绝签发证书、停止证书的使用、撤销证书。由此造成的后果，SZCA 不承担责任。之后 SZCA 及其授权机构会依据内部相关流程规定，对申请做出驳回和受理的决定。申请一经受理，则进入审核环节。

SZCA 和其授权的证书服务机构建议证书订户或者订户代理人妥善保存申请资料和相关证明文件的复印件。

2. 各相关当事人的责任

（1）SZCA的责任

SZCA应保证其CA机构本身的签名私钥得到安全的存放和保护，其建立和执行的安全机制符合国家相关政策的规定。

SZCA应对其授权的证书服务机构进行审计和管理，保证整个申请过程的安全可靠。SZCA亦应保证其整个CA系统安全可靠的运行。由于客观意外或其它不可抗力造成的操作失败或延迟造成的损失、损坏除外。由于技术的进步与发展，SZCA亦有责任提醒证书订户及时更换证书以保证证书的可靠性。

（2）注册机构RA的责任

注册机构RA按照规定程序一经取得SZCA的授权，即有义务遵循SZCA CPS和SZCA的授权运作协议和其它SZCA公布的标准和流程，受理证书服务申请者的证书服务请求，并依据授权设置和管理各类下级证书服务受理机构，包括RA、LRA等。

RA须遵循SZCA制订的《注册机构运营规范》，SZCA将不断的完善并及时对其披露有关的规范和标准内容。RA按照SZCA的要求和规范，确定下属证书服务受理机构的设置方式、管理方式和审核方式，这些方式的确定必须以书面的文件形式告知SZCA，涵盖并且不得与SZCA

规定的相关条款产生冲突、矛盾或者不一致。

RA依据SZCA CPS的规定，有义务确保其运营系统处在安全的物理环境中，并具备相应的安全管理和隔离措施。RA必须能够提供证书服务全部的数据资料及备份，并按照SZCA的要求，保证其与下属证书服务机构间的信息传输安全。重要的是，RA须严格执行为所有证书用户提供资料的义务，并愿意承担因此而带来的法律责任。

SZCA根据SZCA CPS和授权协议对RA进行管理，包括进行服务资质审核和规范执行检查。CA具有对所有证书服务申请者服务请求的最终处理权。CA有权对申请者的资料进行复查；因为RA对申请者的资格审核不严而导致的由证书使用引起的所有损失，由RA承担。

（3） 证书申请者的责任

证书申请者须严格遵守与证书申请以及私钥有关的所有权及安全保存的相关程序：

证书申请者须保证在证书服务申请表上填列的所有声明和信息是完整、准确、真实和可供发证机构查实的；并承担一切因填写虚假信息所造成的法律后果。

证书申请者须了解并遵循SZCA CPS所述条款以及由SZCA推荐使用的安全措施，确保充分了解私钥保存的重要性，确保私钥的安全性。

证书申请者在申请、接受证书及其相关服务前，需要了解SZCA CPS的条例和与证书相关的证书政策，SZCA在接到证书申请者的任何服务申请时即认为该申请者已经了解SZCA CPS的内容，并承诺遵循其中所有相关规定。

证书申请者一旦提交了证书申请，尽管事实上还没有接受证书，但仍被视为该用户已同意发证机构签发其证书。

（4）订户的责任

SZCA一旦通过证书申请者的申请并为其签发证书，无论是否已经接受证书，证书申请者皆被视为SZCA的证书订户。

订户必须确保本身持有的证书用于申请时预定的目的。订户有责任保证私钥的安全。SZCA并不要求证书申请者一定遵从SZCA要求的安全措施；订户可以选择任何自己认为可行的保密措施，并承担所有因用户的私钥保存出现问题而带来的责任。

一旦发生任何可能导致安全性危机的情况，包括证书订户遗失、遗忘私钥或泄密以及其它可能造成损失的情况，证书订户应立刻通知SZCA及其授权的各级证书服务机构，采取申请作废等处理措施，以保证订户的利益。由于通知延误所造成一切损失由证书订户自行承担。

（5）依赖方的责任

依赖方在信赖任何SZCA及其下级操作子CA签发的证书的时候，必须保证遵守以下条款：

依赖方了解SZCA CPS的条款以及和证书相关的证书策略，了解证书的使用目的。

依赖方在信赖SZCA的证书前，有义务查询SZCA公布的最新的CRL，以获得该证书的状态。如CRL显示该证书已作废，则SZCA没有义务继续保证该证书的有效性；SZCA认为，依赖方一直是遵循了此条款的。一旦依赖方因为疏忽或者其它原因违背了此条款而给SZCA带来损失时，SZCA保留追究其法律责任的权利。

所有依赖方对证书的信赖行为即表明他们接受并了解SZCA CPS的有关条例包括有关免责、拒绝和限制义务的条款。

（6） 目录服务的责任

SZCA在目录服务器上发布证书订户的证书公开信息和相关CRL。

SZCA周期性自动发布和更新目录服务和CRL，并会根据有关法律、政策的要求，以及证书服务的要求，进行人工调整；对于这种调整，SZCA将在https://www.szca.com进行公布。

4.2 证书审核

4.2.1 证书申请的识别与鉴定

SZCA 或授权的发证机构遵循本 CP 第三章的规定和相关流程规定对证书申请者提交的 CPS 规定的材料进行审核，决定申请的批准或驳回。

4.2.2 证书申请的批准与驳回

1. 证书申请的批准

SZCA注册机构成功完成了证书申请所有必须的确认步骤并提交证书请求后，SZCA通过发行正式证书来批准证书申请。证书的签发意味着SZCA最终完全正式地批准了证书申请。

2. 证书申请的驳回

SZCA授权的发证机构根据其独立判断，有权拒绝签发证书，并且不对因此而导致的任何损失或费用承担任何责任。如果申请者未能成功通过身份鉴别，SZCA将驳回申请者的证书申请。通常情况下，此类驳回情形以及原因将告知申请人，然而SZCA亦有权在认为必要时拒绝通知申请人相关事由及解释失败原因，并不承担因此而造成的损失赔偿责任。被拒绝的证书申请人可再次提出申请。

4.2.3 证书审核时间

在提交的资料齐全且符合要求的情况下，SZCA 或其授权的发证机构将在 5 个工作日内对申请者提交的申请信息进行审核，若延长，需向申请者说明理由。

4.3 证书签发

4.3.1 证书签发中发证机构和电子认证服务机构的行为

SZCA 批准证书申请后，客户信息通过安全通道发送至 SZCA，SZCA 签发证书并返回给 RA 供下载。与此同时，SZCA 授权的发证机构将有关说明资料提供给用户。

4.3.2 电子认证服务机构和发证机构对订户的通告

SZCA 直接通知订户或发证机构证书已签发。通知方式会因具体情况的不同而有所改变，主要方式有：面对面通知、短信通知、电子邮件通知及其他 SZCA 认为可行的方式。

4.4 证书接受

4.4.1 构成接受证书的行为

在 SZCA 数字证书签发完成后，SZCA 授权的发证机构将会把数字证书及相关资料交给证书申请者，证书申请者从获得证书时起即被视为已接受证书。证书申请者接受数字证书后，应妥善保存其证书对应的私有密钥。

4.4.2 SZCA 对证书的发布

SZCA 签发完成的证书将自动发布到目录服务器中，供订户和依赖方查询和下载。

4.4.3 SZCA 对其他实体的通告

对于 SZCA 的证书签发行为，SZCA 及其授权注册机构不对其他实体进行通告。

4.5 密钥对与证书的使用

4.5.1 订户私钥和证书的使用

订户接受数字证书后，必须妥善保存与其证书对应的私有密钥，避免遗失、泄漏、被篡改或者被盗用。任何使用者使用证书时都必须检验证书的有效性，包括该证书是否被撤销、是否在有效期内、是否是 SZCA 和其授权的发证机构签发等。

订户只能在指定的应用范围内使用私钥和证书，订户只有接受了相关证书之后才能使用对应的私钥，并在证书到期或被撤销之后，订户必须停止使用私钥。

4.5.2 依赖方公钥和证书的使用

在依赖方接受数字签名信息后需要：

- 获得数字签名对应的证书及信任链；
- 确认该签名对应的证书是依赖方信任的证书；
- 证书的用途适用于对应的签名；
- 使用证书上的公钥验证签名；
- 确认数字签名对应的证书状态正常，没有进入 CRL 列表。

依赖方需要采用合适的软（硬）件进行数字签名的验证工作，包括验证证书链及链中所有证书的数字签名。

4.6 证书更新

4.6.1 证书更新的情形

SZCA 会为签发的证书设置有效期，有效期从签发之日起开始计算，一般为一年。当订户证书即将到期或已经到期时如需证书密钥更新的，应于证书有效期届满前 1 个月内申请，由证书的订户、证书订户的授权代理（机构证书）或证书对应实体的拥有者（设备证书）申请更新证书。

在证书有效期内，证书订户的旧加密密钥丢失或损坏的情况下可以申请证书更新。证

书更新的规定与证书密钥更新的相同。

4.6.2 请求证书更新的实体

参照本 CP4.1.1。

4.6.3 证书更新请求的处理

在对订户证书进行更新前，必须确认证书更新请求是被更新证书的订户（或订户授权的代理）提出的，例如：要求订户提交初始登记时候提供的鉴别信息（或者等同的方式），或要求证书更新申请者提交原证书中公钥对应的私钥的签名。处理证书更新请求可与初始证书申请的鉴别方式相同。

审核通过 SZCA 签发新证书且订户接受后，SZCA 吊销旧证书。

4.6.4 颁发新证书时对订户的通告

参照本 CP4.3.2。

4.6.5 构成接受更新证书的行为

参照本 CP4.4.1。

在订户在线或离线递交更新请求获得批准后，就意味着申请者已经表示接受了更新证书。SZCA签发证书后将按照订户申请证书更新的方式向其发布证书。

4.6.6 电子认证服务机构对密钥更新证书的发布

密钥更新后的证书会在更新的同时被 CA 机构发布到公开的信息库和指定的数据库中。新证书签发后，旧的证书将被注销。SZCA 在目录服务器 LDAP 上发布用户新证书。用户旧证书通过 CRL 发布。

4.6.7 电子认证服务机构对其他实体的通告

参照本 CP4.4.3。

4.7 证书密钥更新

证书密钥更新即产生新的密钥对，使用与原证书一样的主题甄别名签发新证书。 证书到期更新证书的，发证机构默认的安全方式是同时自动更新证书密钥。

4.7.1 证书密钥更新的情形

如出现下列情形的,订户必须选择证书密钥更新：

- 证书到期并且密钥对的有效期也到期(最终订户的私有密钥有效期一般均与其证书的有效期一致）。

- 密钥对已经被泄漏、被窃取、被篡改或者其它原因导致密钥对安全性无法得到保障。

- 证书被撤销后需要重新获得证书。

此外，凡是在SZCA运营体系架构内部使用的证书，包括RA、服务操作人员等的证书到期后，必须进行证书密钥更新。

证书即将到期的订户，出于安全考虑，应尽量采取证书密钥更新，获得新的证书。

4.7.2 请求证书密钥更新的实体

参照本 CP4.1.1

4.7.3 证书密钥更新流程

1.解密证书加密文件，删除证书

订户在进行密钥更新之前将加密邮件等加密过的文件进行解密，同时备份（例如将邮件内容复制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密钥的更新。(如订户未解密文件而进行密钥更新，由此造成的可能损失，SZCA 概不负责)；

2.发起密钥更新请求

订户或其授权代理人提交密钥更新请求，并书面填写《数字证书申请表》。

3.SZCA 审核处理

电子认证服务机构在对订户证书进行密钥更换前，需要确认密钥更换请求是被更换证书

的订户（或订户授权的代表）提出的，例如：要求订户提交登记时候提供的鉴别信息（或者等同的方式），或要求密钥更换申请者提交原证书中公钥对应的私钥的签名。用于原始证书申请的鉴别也可以用于处理密钥更换请求。

如果订户证书对应的私钥发生泄露，电子认证服务机构必须采用初始证书申请的鉴别流程来处理密钥更换请求。

审核通过后，SZCA 签发莘泽行数交给订户，旧证书自动吊销，并通过 CRL 发布。

4.7.4 颁发新证书时对订户的通告

参照本 CP4.3.2。

4.7.5 构成接受密钥更新证书的行为

参照本 CP4.6.5。

4.7.6 电子认证服务机构对密钥更新证书的发布

参照本 CP4.6.6。

4.7.7 电子认证服务机构对其他实体的通告

参照本 CP4.4.3。

4.8 证书变更

4.8.1 证书变更的情形

在证书有效期内，当证书中包含的用户信息（除公钥外）发生变化时，订户可以通过证书变更获得新证书。证书的变更将被视为初始的证书申请。SZCA 将吊销原证书，后签发新证书。证书变更的申请、处理流程与申请新证书的流程相同。

4.8.2 请求证书变更的实体

参照本 CP4.1.1。

4.8.3 证书变更请求的处理

订户按照原申请证书的流程，到发证机构填写《数字证书申请表》，发证机构按照原证书申请流程对证书变更申请进行身份鉴别和审核，发证机构确认并批准变更申请后，为其签发新的证书，该证书的公钥为申请者原有的公钥。

证书变更后，证书的有效期并没有改变，仍然为原证书的有效期。

4.8.4 颁发新证书时订户的通告

参照本 CP4.3.2。

4.8.5 构成接受证书变更的行为

参照本 CP4.6.5。

4.8.6 电子认证服务机构对变更证书的发布

参照本 CP4.6.6。

4.8.7 电子认证服务机构对其它实体的通告

参照本 CP4.6.7。

4.9 证书吊销和挂起

证书吊销是永久性吊销，不可以进行证书恢复。

4.9.1 证书吊销的情形

发生下列情形，订户证书必须被吊销：

1. 新的密钥对替代旧的密钥对；

2. 密钥失密：与证书中的公钥相对应的私有密钥被泄密或用户怀疑自己的密钥失密；

3. 从属关系改变：与密钥相关的订户的主题信息改变，证书中的相关信息有所变更；

4. 操作终止：由于证书不再需要用于原来的用途，但密钥并未失密，而要求终止（例如订户离开了某个组织）；

5. 证书的更新费用未收到；

6. 订户主体不存在；

7. 订户不能遵守 SZCA CPS 或其它协议、法律及法规所规定的责任和义务；

8. 订户申请初始注册时，提供不真实材料；

9. 证书已被盗用、冒用、伪造或者篡改；

10. CA 失密：电子认证服务机构因运营问题，导致 CA 内部重要数据或 CA 根密钥失密等原因；

11. 订户申请撤销；

12. 其它情形。

4.9.2 请求证书吊销的实体

在符合本CP4.9.1的第1～10条的情形下，请求证书撤销的实体可以是SZCA也可以是其授权发证机构或子CA，构成强制撤销，撤销后必须立即通知该订户。

在符合本CP4.9.1的第11条的情形下，请求证书撤销的实体与本CP4.1.2所述一致。

其他情形视具体情况而定，SZCA在此有酌情权。

4.9.3 证书吊销的流程

1.订户申请撤销流程如下：

- 订户在申请证书撤销之前将加密邮件等加密过的文件进行解密，同时备份（例如将邮件内容复制以明文方式存储或将邮件附件保存），然后将证书删除。
- 申请者到 SZCA 及授权注册机构书面填写《数字证书申请表》，并注明撤销的原因，提交身份证明材料；
- SZCA 及授权注册机构遵循本 CP3.2.2 或 3.2.3 对订户身份进行鉴别，并按 CP3.4 对订户提交的证书撤销申请进行查验；

- SZCA 及授权注册机构核验通过后吊销证书。
- SZCA 将信息及时发布于信息库供查询。

2. 强制撤销：

SZCA授权的发证机构可以对订户的证书进行强制撤销，撤销后必须立即通知该订户。强制撤销的命令来自于：SZCA或SZCA授权的发证机构；SZCA撤销订户证书后，发证机构将书面或短信通知订户证书被撤销，并通过CRL向外界公布。

4.9.4 吊销请求宽限期

一旦发现需要吊销证书，订户应该实时提出吊销请求，如果确实因为客观原因导致延迟的，这个时间也不得超过 8 个小时。如果在宽限其内，因订户未及时提出吊销请求而产生的任何损失和责任，SZCA 并不承担。

4.9.5 电子认证服务机构处理吊销请求的时限

通常情况下，SZCA 授权证书服务机构在接到客户吊销请求后，48 个小时内能够完成证书吊销流程，并在 CRL 上公布。

4.9.6 依赖方检查证书吊销的要求

依赖方应经常检查CRL，包括：

- 在认证各方的数字证书前，根据SZCA最新公布的CRL检查该证书的状态；
- 在使用证书前根据SZCA最新公布的CRL检查证书的状态；
- 验证CRL可靠性和完整性，确保它是经SZCA发行并电子签名的。

依赖方应根据SZCA公布的最新CRL确认使用的证书是否被撤销。如果CRL公布证书已经撤销，而依赖方没有查CRL，由此造成的损失由依赖方承担。

4.9.7 CRL 发布频率

SZCA 证书吊销列表在 24 小时内自动变更，特殊紧急情况下可以通过手动方式变更 CRL 列表。

4.9.8 CRL 发布的最大滞后时间

CRL 发布的最大滞后时间为 24 小时。

4.9.9 在线的吊销/状态查询的可用性

SZCA 提供在线的吊销/状态查询，该服务 7X24 小时可用。

4.9.10 在线的吊销查询要求

SZCA OCSP 系统查询没有设置任何读取权限。

4.9.11 吊销信息的其他发布形式

除 CRL 与 OCSP 之外，尚无其它发布形式。

4.9.12 针对密钥泄露的特殊要求

无论是最终订户还是 SZCA、授权注册机构，发现证书密钥受到安全损害时应立即吊销证书。

4.9.13 证书挂起

证书用户暂停使用证书及其它原因，可以申请证书挂起。SZCA或SZCA授权的发证机构也有权在认为必要时，执行强制挂起，强制挂起后必须立即通知该订户。 证书挂起期间用户不能正常使用用户证书。

4.9.14 请求证书挂起的实体

参照本 CP4.1.1。

4.9.15 证书挂起流程

- 申请者到SZCA授权的发证机构书面填写《数字证书申请表》， 勾选“冻结”项，并注

明挂起的原因；

- SZCA授权的发证机构遵循本CP3.3规定对订户提交的证书挂起申请进行查验；

- 强制挂起：SZCA授权的发证机关管理员可以依法对订户证书进行强制挂起，挂起后必须立即通知该订户。强制挂起的命令来源于：SZCA或SZCA授权的发证机构；

- SZCA挂起订户证书后，发证机构将当面通知或通过各种有效途径（电话、电子邮件、书面、传真等）通知订户证书已被挂起；

- 订户证书被挂起后，订户必须在证书有效期到期前恢复证书。SZCA将努力通过各种有效途径（电话、电子邮件、书面文字、传真等）提醒订户，若证书到期订户还是没有回复，SZCA或SZCA授权的发证机构有权自行撤销证书。对此造成的任何后果， SZCA不承担任何责任。

4.9.16 挂起的期限限制

订户需在证书到期前对挂起的证书进行恢复。

4.9.17 挂起证书的恢复流程

挂起证书恢复的具体流程如下：

- 申请者到SZCA授权发证机构书面填写《数字证书申请表》，勾选“解冻”项；

- SZCA授权的发证机构遵循本CP3.3所述对订户提交的证书恢复申请进行查验；

- 发证机构审核通过后，为订户恢复证书。并通知订户证书已被恢复；

- 订户得到恢复通知，证书恢复完成。

4.10 证书状态服务

4.10.1 操作特征

SZCA提供两种状态查询服务：

1. CRL

CRL通过LDAP发布服务器进行发布，其可信度及安全性由根证书的签名来保证。订户需要将CRL下载到本地后进行验证，包括CRL的合法性验证和检查CRL中是否包含待检验证书的序列号。

2. OCSP

SZCA提供OCSP（在线证书状态查询服务协议）服务，订户可以通过访问SZCA网站 https://www.szca.com 获得证书的状态信息。

4.10.2 服务可用性

SZCA 提供 7X24 小时不间断证书状态查询服务。

4.11 服务终止

服务终止是指证书使用者终止与 SZCA 的服务，它包含以下两种情况：证书到期时终止与 SZCA 的服务和证书未到期时终止与 SZCA 的服务。

4.12 密钥生成、备份与恢复

4.12.1 签名密钥的生成、备份与恢复的策略与行为

订户签名密钥对由订户的密码设备生成，其中签名密钥中的私钥从技术上做到不能复制，确保订户签名私钥的安全性和唯一性。因此订户须妥善保管，由签名私有密钥遗失所造成的损失由订户自己承担。

SZCA 不支持恢复订户签名私钥。

4.12.3 加密密钥的生成、备份和恢复的策略和行为

证书订户的加密密钥由国家设立的专门的深圳市密钥管理中心生成，并由其进行备份。在如下情形下允许进行密钥的恢复：

1. 由于加密密钥丢失或其他原因，订户需要进行证书恢复的情形

按照深圳市密钥管理中心相关规定、流程，接受订户的加密密钥恢复申请，为订户进行加密密钥的恢复。

2. 国家执法机关、司法机构因执法、司法或国家其它管理部门管理或取证的需要

只有在特定的情况下遵照国家相关法律的情况下才能进行此类密钥回复。申请要提出充分的理由和提供有关文件、材料。

3. 深圳市密钥管理中心认为有必要。

不在此规定。

第五章 设施、管理和运作控制

此章节与CPS内容相同。

第六章 认证系统技术安全控制

此章节与CPS内容相同。

第七章 证书、CRL 和 OCSP

7.1 证书

SZCA 证书格式采用的是 ITU-T 推荐的国际标准。

7.1.1 版本号

SZCA 订户证书，符合 X.509 V3 证书格式。

7.1.2 证书标准项

表 7.1—证书标准项

域	值或值的限制
证书版本号（version）	指明 X.509 证书的格式版本，值为 V3
序列号（serial number）	即由 SZCA 分配给证书的唯一的数字型标识符
签名算法（signature）	指定由 SZCA 签发证书时所使用的签名算法
签发者 DN	用来标识签发证书的CA的X.500 DN名字 CN = SZCA

	OU = szca O = ShenZhen Certificate Authority L = Shenzhen S = Guangdong C = CN
有效期（validity）	用来指定证书的有效期，包括证书开始生效的日期和时间以及失效的日期和时间。每次使用证书时，需要检查证书是否在有效期内
证书主题（subject）	指定证书持有者的 X.500 唯一名字。包括国家、省、市、组织机构、单位部门和通用名，还可包含 E-mail 地址等个人信息等
公钥	证书持有者公开密钥信息域包含两个重要信息：证书持有者的公开密钥的值；公开密钥使用的算法标识符。此标识符包含公开密钥算法和 hash 算法。
微缩图算法	SZCA 对证书内容的签名算法。
微缩图	SZCA 对证书内容的签名值

7.1.3 证书扩展项

SZCA 除了使用证书标准项和标准扩展项以外，还使用 SZCA 规定的自定义扩展项。见表 7.2 和表 7.3。

1.证书扩展项

表 7.2-证书扩展项

域	值或值的限制
颁发机构密钥标识符	此域用在当同一个 X.500 名字用于多个认证机构时，用来唯一标识签发者的 X.500 名字
主题密钥标识符	此域用在当同一个 X.500 名字用于多个证书持有者时，用来唯一标识证书持有者的 X.500 名字
密钥使用	指定各种密钥的用法：电子签名，不可抵赖，密钥加密，数据加密，密钥协议，验证证书签名，验证 CRL 签名，只加密，只解密，只签名
CRL 发布点	由 SZCA 定义的 CRL 发布点

2. 自定义扩展项

针对不同的证书应用服务，SZCA 自定义扩展项。

表 7.3-自定义扩展项

域	值或值的限制
企业标识	指定企业的唯一标识符
组织机构代码	此域用来记录机构的组织机构代码
注册号	指定机构、企业的注册号
CRL 发布点	由 SZCA 定义的 CRL 发布点。
登记机关	指定机构、企业的登记机关
法人(负责人)	指定机构、企业的法人(负责人)名称
法人身份证号	指定机构、企业的法人(负责人)身份证号
岗位名称	指定机构、企业内工作岗位的名称
机构签名证书序列号	指定机构、企业证书中签名证书序列号
业务属性	指定机构/企业业务证书所适用的业务属性
扩展代码	指定机构/企业业务证书颁发的数量
岗位责任人	指定机构/企业业务证书中所在岗位的责任人
岗位责任人身份证号	指定机构/企业业务证书中所在岗位的责任人身份证号

7.1.4 密钥算法对象标识符

SZCA 签发的证书中，密码算法的标识符为 RSAsha128、RSAsha256 和 SM2 三种。

7.1.5 命名形式

SZCA 证书，其命名形式的格式和内容符合 X.501 的甄别名格式。详见本 CP3.1 节。

7.1.6 命名限制

SZCA 签发的证书，其识别名称不允许匿名或者伪名，必须是有确定含义的识别名称。

7.1.7 证书策略对象标识符

SZCA 按照 X.509 标准签发的证书，其证书策略对象标识符，存放在证书内证书策略的相关栏目。具体请参考附录中的证书格式规范。

7.2 CRL 描述

SZCA 定期签发 CRL，供用户查询使用。SZCA 签发的 CRL 符合 RC3280 标准。

7.2.1 版本号

SZCA 目前签发 X.509 V2 版本的 CRL，此版本号存放在 CRL 版本格式栏目内。

7.2.2 CRL 和 CRL 条目扩展项

此章节与CPS内容相同。

7.2.3 CRL 下载

可以通过 SZCA 网站 https://www.szca.com，或证书中签发的 CRL 扩展项标明的 URL 下载 CRL。

7.3 OCSP

SZCA 为用户提供 OCSP，OCSP 作为 CRL 的有效补充，方便证书用户及时查询证书状态信息。

7.3.1 OCSP 请求

此章节与CPS内容相同。

7.3.2 OCSP 响应

此章节与 CPS 内容相同。

7.3.3 OCSP 扩展项

此章节与 CPS 内容相同。

第八章 合规性审计和其他评估

SZCA 无条件接受信息产业主管部门的审计检查与评估，并对审计检查中发现的问题进行及时的整改。

SZCA 内部定期对物理控制、密钥管理、操作控制、鉴证执行等情况进行审查，以确定实际发生情况是否与预定的标准、要求一致，并根据审查结果采取行动。

8.1 评估的频度和情形

外部评估：由主管部门根据相关法律法规或最新安全形势要求决定。

内部评估：定期或不定期，但频率通常为每年一次，特殊情况除外。

8.2 评估者的身份/资格

内部审计由 SZCA 内部人员组成；外部审计由具有相关资质的第三方审计机构进行审计。

8.3 评估者与被评估者之间的关系

评估者与被评估者必须无任何业务、财务等利益关系，或者其它任何利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对 SZCA 进行评估。

8.4 评估的内容

评估内容主要包括人事、物理环境建设、安全运营管理、系统结构及运营服务、密钥安全管理、客户服务、证书处理流程等。

8.5 对问题与不足采取的行动

此章节与 CPS 内容相同。

8.6 评估结果的传达与发布

此章节与 CPS 内容相同。

第九章 法律责任和其他业务条款

此章节与 CPS 内容相同。