深圳 CA 证书策略

（CP）

V2.0

2021 年 12 月

https://www.szca.com

版本信息

文档	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 年 6 月 25 日	证书策略发展小组	安全策略管理委员会	首次制定发布
V2.0	2021 年 12 月 29 日	证书策略发展小组	安全策略管理委员会	补充第 5、6、9 章节具体内容的描述

目录

1. 概括性描述

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

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

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

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

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。

1.3.5 证书申请者

任何期望成为 SZCA 或其下级子 CA 的订户的实体，都可以成为 SZCA 的证书申请者，根据其想要获得的证书类型，按照本 CPS 的规定提供必要的材料、信息，完成申请过程。

1.3.6 其他参与者

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。

此外，证书不设计用于、不打算用于、也不授权用于危险环境中的控制设备，或用于要求防失败的场合，如核设备的操作、航天飞机的导航或通讯系统、空中交通控制系统或武器控制系统中，因为它的任何故障都可能导致死亡、人员伤害或严重的环境破坏。

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 运营安全管理小组，当需要修订 CP 时，由安全运营管理小组牵头组织技术中心、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 运营安全管理小组审核并发布。

1.5.2 联系人

如对本 CP 有任何疑问，请联系 SZCA 运营安全管理小组：

电话：0755-26588399

传真：0755-86156366

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 运营安全管理小组”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 运营安全管理小组审核。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 运营安全管理小组批准，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 运营安全管理小组在 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 运营安全管理小组”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 运营安全管理小组	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 电子认证业务规则 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

2.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。

3.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或进行其他法人的身份认证、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，并填写完整申请材料（如申请表、服务协议）：
   - 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、合格证（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。

3.2.6 不需验证的订户信息

无规定。

3.2.7 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。

3.2.8 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。

4.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”将申请材料填写完整，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材料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，并提交申请材料填写。

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 签发新证书交给订户，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，向发证机构提交数字证书申请材料，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。
- 申请者向 SZCA 及授权注册机构提交数字证书撤销申请材料，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

- 申请者向SZCA授权的发证机构提交数字证书申请材料，申请证书冻结，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：

- 申请者向SZCA授权发证机构提交数字证书挂起的申请材料，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，由用户自行保管。

SZCA不保管、恢复订户签名私有密钥，以保证订户签名私钥的安全性和唯一性。因此，提醒并要求订户妥善保管。由于签名私有密钥遗失所造成的损失由订户自己承担，SZCA概不负责。

密钥管理中心密钥无法恢复订户签名密钥。

4.12.2 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。

5.设施、管理和运作控制

5.1 物理控制

SZCA 的认证服务系统位于安全稳固的建筑物内，具备独立的软硬件操作环境。只有经过授权的操作人员，才可以根据有关的安全操作规范进入相应的管理区域进行操作。SZCA 的根密钥位于最高安全强度的环境内，避免被破坏或者被未经授权的操作。

5.1.1 场地位置与建筑

SZCA 认证系统的主机房位于深圳市南山区高新中二路深圳软件园 8 栋三楼，机房按照功能分为业务受理区、辅助设备区、服务区、RA 管理区、CA 管理区、CA 核心区、KM 管理区、KM 核心区。具备了抗震、防火、防水、恒湿温控、防电磁干扰与辐射、备用电力、门禁控制、视频监控等功能以保证认证服务的连续性和可靠性。

5.1.2 物理访问

操作人员进入机房，必须通过 IC 卡门禁系统和指纹识别系统的身份检验，并有 24 小时视频监控设备。

操作人员进入具体工作区域进行操作，必须通过该区域指纹验证和权限检验，并且所有的操作过程都进行记录。

5.1.3 电力与空调

SZCA 系统采用双电源供电，在单路电源中断时，可以维持系统正常运转。同时，使用不间断电源（UPS），避免电源波动也保障紧急情况的供电。

系统机房使用中央空调,进行温度和湿度的调控。采用两部独立空调互为备份的方式运作，机房安置了新风系统，对机房进行换气，保证机房内的空气品质、温湿度和新风供应以及机房对空气清洁度的要求等均达到国家规定的标准。

5.1.4 水患防治

SZCA 的机房位于大楼三楼，认证服务系统所处的环境为密闭式建筑，并且安装了水浸自动报警系统等预防水浸措施，充分保障系统安全。

5.1.5 火灾防护

SZCA 机房内安装了火灾自动报警系统及气体自动灭火系统，该系统具有自动、手动及机械应急操作三种启动方式。在自动状态下，当防护区发生火警时，火灾报警控制器接到防护区两个独立火灾报警信号后立即发出联动信号。经过 30 秒时间延时，火灾报警控制输出信号，启动灭火系统，同时，报警控制器接收压力讯号器反馈信号，防护区内门灯显亮，避免人员误入。当防护区经常有人工作时，可以通过防护区门外的手动/自动转换开关，使系统自动状态转换到手状态，当防护区发生火警时，报警控制器只发出报警信号，不输出动作信号。由值班人员确认火警，按下控制面板或击碎防护区外紧急启动按钮，即可立即启动系统，喷发气体灭火剂。当自动、手动紧急启动都失灵时，可进入储瓶间内实现机械应急操作启动。

5.1.6 介质存储

SZCA 对重要介质的存放和使用满足防火、防水、防震、防潮、防腐蚀、防虫害、防静电、防电磁辐射等的安全需求。采取了介质使用登记注册、介质防复制及信息加密等措施实现了对介质的安全保护。

5.1.7 报废处理

SZCA 的认证服务系统使用的硬件设备、存储设备、加密设备等，当废弃不用时，涉及敏感性和机密性的信息都被安全、彻底的消除。密码设备在作废处置前根据制造商的指南将其物理销毁或初始化。

文件和存储介质包含有敏感性和机密性信息时，在处理时都经过了特殊的销毁措施，保证其信息无法被恢复和读取。

所有处理行为将记录在案，以供审查的需要，所有的销毁行为遵守我国有关的法律法规。

5.1.8 异地备份

SZCA 对重要数据进行异地备份，遇到灾难情况发生时保证数据安全。

5.2 程序控制

5.2.1可信角色

电子认证服务机构、注册机构、依赖方等组织中与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，必须由可信人员担任。

为确保责任明确，建立有效的安全机制，保证内部管理和操作的安全，SZCA 明确可信角色包括但不限于以下职位：

- SZCA运营安全管理小组
- SZCA超级管理员
- SZCA系统管理员
- 系统审计员
- 密钥管理员
- 安全管理员
- 网络管理员
- 监控管理员
- 门禁管理员
- 录入员
- 审核员
- 制证员

安排这些职位是为了确保责任明确，建立有效的安全机制，保证内部管理和操作的安全。

5.2.2 每项任务需要的人数

表 5.1-可信角色最低人数配备

序号	可信角色	人数
1	运营安全管理小组	3-5
2	超级管理员	2
3	系统管理员	2
4	系统审计员	1
5	安全管理员	1
6	网络管理员	1
7	监控管理员	1
8	门禁管理员	1
9	密钥管理员	1
10	录入员	若干
11	审核员	若干
12	制证员	若干

5.2.3每个角色的识别与鉴别

所有 SZCA 的在职人员，根据所担任角色的不同进行身份鉴别。SZCA 根据各角色作业性质和职位权限，发放需要的系统操作卡、门禁卡、登录密码、操作证书等安全令牌。对于使用安全令牌的员工，SZCA 系统将独立完整地记录并监督其所有的操作行为。

所有 SZCA 关键职位人员必须确保：

1. 发放的安全令牌只直接属于个人或组织所有

2. 发放的安全令牌不允许共享

3. SZCA 的系统和程序通过识别不同的令牌，对操作者进行权限控制

5.2.4 需要职责分割的角色

为确保系统安全，遵循可信角色权限分割、操作和审计分离的原则，SZCA 的可信角色均由不同的人担任。

在 SZCA 定义的可信角色中，安全管理员和网络管理员不能由同一人担任；系统管理员和网络管理员不能由同一人担任；系统管理员和系统审计员不能由同一人担任；监控管理员和门禁管理员不能由同一人担任；录入员和审核员不能由同一人担任。

至少两个人以上才能使用一项对参加操作人员保密的密钥分割或合成技术，来进行任何密钥的恢复工作。

5.3 人员控制

5.3.1资格、经历和无过失要求

SZCA 与所有员工签订保密协议，成为SZCA 可信角色的人员必须提供相关的教育背景、资历证明，并具有足以胜任其工作的相关经验，且没有相关的不良记录。

SZCA 对承担可信角色的工作人员应具备的基本条件如下：

1. 具备良好的社会和工作背景；

2. 遵守国家法律、法规，服从 SZCA 的统一安排及管理；

3. 遵守 SZCA 有关安全管理的规范、规定和制度；

4. 具有良好的个人素质、修养以及认真负责的工作态度；

5. 具备良好的团队合作精神。

5.3.2背景审查程序

SZCA 员工的录用须经过严格的可信背景调查，且需要有不少于 3 个月的试用期，未通

过初次背景调查的员工，一律不得录用。可信人员背景调查及信誉度调查定期进行，原则上 3 年一次，SZCA 根据实际情况可增加调查次数。

背景调查分为基本调查和高级调查。

1）基本调查包括身份验证、工作经历、职业推荐、教育水平和身体状况方面的调查。

2）高级调查除包含基本调查项目外，还包括对信用情况、犯罪记录、社会关系和社会安全方面的调查

调查程序包括：

1）人事部门负责对应聘人员的个人资料予以确认。提供以下资料：个人履历、最高学历证明、资格证及身份证等相关有效证明。

2）人事部门通过电话、网络、信函和走访等形式对应聘人员所提供材料的真实性进行鉴定。

3）用人部门通过日常观察、现场考核和情景考验等方式对人员进行考察。

注册机构、注册分支机构和受理点操作人员的审查也必须参照 SZCA 可信人员调查制度对其进行考察。受理点责任单位可以在此基础上，增加调查、试用和培训条款，但不得违背 SZCA 证书受理的规程和 SZCA 电子认证业务规则。

劳动合同关系存续期间或员工离职日起 2 年内仍然不得从事与 SZCA 相类似的工作。

SZCA 员工的录取按照招聘制度规定程序经过严格的审查，根据岗位需要增加相应可信员工的背景调查。通常情况下，新进员工需要有试用期。根据试用的结果安排相应的工作或者辞退。

SZCA 对其关键的 CA 员工进行严格的背景调查。调查内容包括但不限于验证先前工作记录；验证身份证明真实性；验证学历、学位及其他资质证书的真实性；验证无其他不诚实行为等。注册机构、注册分支机构和受理点操作员的审查亦参照 SZCA 对可信员工的调查方式。受理点责任单位可以在此基础上，增加调查、试用和培训条款，但不得违背 SZCA 证书受理的规程和 SZCA 电子认证业务规则。

SZCA 确立流程管理规则，据此 CA 员工受到合同和章程的约束，不许泄露 SZCA 认证服务体系的敏感信息。所有的员工与 SZCA 签订保密协议，合同期满以后 2 年内仍然不得

从事与 SZCA 相类似的工作。

根据具体情况 SZCA 会与有关部门或调查机构合作，完成对 SZCA 可信员工的背景调查。

5.3.3培训要求

SZCA 根据需要对员工进行职责、岗位、技术、政策、法律、安全等方面的培训。SZCA 对 SZCA 员工提供包括但不限于以下内容的综合性培训：

- 公司文化及各类管理制度；
- 安全管理制度；
- 专业知识培训；
- 岗位职责及岗位技能培训；
- 相关法律、管理办法等。

5.3.4再培训周期和要求

根据 SZCA 内外部环境的变化及员工自身的状况，SZCA 将对员工进行周期性培训，以适应新的变化，不断提高员工专业素养。具体计划由各部门提报需求，人事部统一安排。

5.3.5工作岗位轮换周期和顺序

SZCA 根据自身需要安排工作轮换，轮换周期视具体情况而定。

5.3.6未授权行为的处罚

当 SZCA 员工进行了未授权或越权操作，SZCA 立即作废或终止该人员的安全证书和 IC 卡。在行为确认后根据情节严重程度，实施包括提交司法机关处理等措施。

5.3.7独立合约人的要求

SZCA 因为人力资源不足或者特殊需要，聘请专业的第三方服务人员参与系统维护、设

备维护等，除了必须就工作内容签署保密协议以外，该服务人员必须在 SZCA 专人全程监督和陪同下从事相关工作。同时还需要对其进行必要的知识培训和安全规范培训，使其能够严格遵守 SZCA 的规范。

5.3.8提供给员工的文档

在培训或再培训期间，SZCA 提供给员工的培训文档包括但不限于以下几类：

1、SZCA 员工手册；

2、SZCA 电子认证业务规则；

3、SZCA 技术体系文档；

4、SZCA 安全管理制度等。

5.4 审计日志程序

5.4.1记录事件的类型

SZCA 的 CA 和 RA 运行系统，记录所有与系统相关的事件，以备审查。它们包括但不限于：

1. CA密钥生命周期内的管理事件，包括密钥生成、备份、恢复、归档和销毁。

2. RA系统记录的证书订户身份信息，包括企业（个人）姓名、证件号码、地址、邮箱、联系人等信息。

3. 证书生命周期的各项操作，包括证书申请、证书密钥更新、证书撤销等事件。

4. 系统、网络安全记录，包括入侵检测系统的记录、系统日常运行产生的日志文件、系统故障处理单、系统变更单等。

5. 系统巡检记录。

6. 人员访问控制记录

这些记录，无论是手写、书面或电子文档形式，都包含事件日期、事件的内容、事件的发生时间段、事件相关的实体等。

SZCA 记录其它与 CA 系统本身不相关的事件，例如：物理通道参观记录、人事变动等。

5.4.2 处理日志的周期

SZCA 每月对记录进行审查，对审查记录行为备案。

5.4.3 审计日志的保存期限

SZCA 审计日志在线记录至少保存 1 个月，离线存档至少 7 年。

5.4.4 审计日志的保护

SZCA 执行严格的通道管理，确保只有 SZCA 授权的人员才能接近这些审查记录。这些记录处于严格的保护状态，严格禁止未经授权的任何访问、阅读并禁止任何修改和删除等操作。

5.4.5 审计日志备份程序

SZCA 保证所有的审查记录和审查总结都按照 SZCA 备份标准和程序进行。根据记录的性质和要求，采用在线和离线的各种备份工具及各种形式的备份。

5.4.6 审计收集系统

应用程序、网络和操作系统等都会自动生成审计数据和记录信息。

5.4.7 对导致事件实体的通告

对审计收集系统中记录的事件，对导致该事件的个人、机构等主体，SZCA 不进行通告。

5.4.8 脆弱性评估

在认证系统运行时，SZCA 从内部和外部对系统可能造成的威胁进行评估，并根据日志的日常审计和监督实施，随时调整和系统运行密切相关的安全控制措施，以便将系统运作的风险降到最低。

5.5 记录归档

5.5.1 归档记录的类型

SZCA 存档的内容包括 SZCA 发行的证书、 CRL、审查数据记录、证书申请审批资料等。

5.5.2 归档记录的保存期限

SZCA 的订户证书及其申请资料存档期限为：证书失效后 5 年。

5.5.3 归档文件的保护

SZCA 对各种电子、磁带、纸质形式的归档文件，都有安全的物理和逻辑保护措施和严格的管理程序，确保归档了的文件不会被损坏，防止非授权的访问、修改、删除或其它的篡改行为。

5.5.4 归档文件的备份程序

所有存档文件的数据库保存在 SZCA 的存储库中。存档的数据库采取物理或逻辑隔离的方式，与外界不发生信息交互。只有授权的工作人员才能在被监督的情况下，对档案进行读取操作。SZCA 在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

5.5.5 记录时间戳要求

所有 5.5.1 条款所述的存档内容都加时间标识。

5.5.6 归档收集系统

SZCA 档案的收集系统由人工操作和自动操作两部分组成。

5.5.7 获得和检验归档信息的程序

SZCA 定期验证存档信息的完整性。

5.6 电子认证服务机构密钥更替

当 CA 根密钥对累计寿命超过本 CP6.3.2 中规定的最大有效期时，SZCA 将启动密钥更新流程。旧的 CA 密钥对到期前，SZCA 将用新的 CA 密钥对签发证书。

5.7 损害与灾难恢复

当 SZCA 遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等情形或因不可抗力造成 SZCA 机房无法正常提供服务时，SZCA 将依照《SZCA 灾难恢复计划》实施恢复。

5.7.1事故和损害处理程序

SZCA 遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，SZCA 将按照《SZCA 应急管理方案》进行处理，必要时启动备份系统。

5.7.2计算资源、软件或数据的损坏

当认证系统运营使用的软件、数据或者其它信息出现异常损毁时，可以依照《SZCA 灾难恢复计划》进行处理。根据系统内部备份的资料，执行系统恢复操作，使认证系统能够重新正常运行。

5.7.3实体私钥损害处理程序

SZCA 的根私钥及 SZCA 下级操作子 CA 证书的私钥出现损毁、遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时：《SZCA 根私钥泄露紧急处理流程》的相关程序进行处理。

5.7.4灾难后的业务连续性能力

SZCA 在遭遇本节 5.7.1 和 5.7.2 中描述的灾难后，将启动《SZCA 灾难恢复计划》，在最短的时间内恢复各项业务的正常运行。

5.8 电子认证服务机构或注册机构的终止

当 SZCA 及其授权服务机构需要终止经营时，将会严格按照《电子认证服务管理办法》第四章（第二十三条至第二十七条）之规定执行。

6.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

- 加密密钥对：加密密钥对是由中华人民共和国国家密码管理局（以下简称国家密码管理局）许可的、SZCA数字证书签发系统支持的KMC产生。

- 签名密钥对：选择硬介质证书订户的签名密钥对由用户端产生，证书申请者可使用深圳市国家密码管理委员会办公室认可的、SZCA数字证书签发系统支持的介质生成签名密钥对。签名密钥存储在介质中不可导出，保证SZCA无法复制签名密钥对。选择软介质证书订户的签名密钥，由SZCA后台密码设备生成，离散加密存储，并保障订户密钥存储及传输的安全。

6.1.2 私钥传送给订户

硬介质证书订户的签名密钥对由自己的密码设备生成并保管。

加密密钥对由 KMC 产生，并通过符合国家密码管理局许可的通讯协议传到订户手中的密码设备中。

软介质证书订户的签名密钥，由 SZCA 离散加密存储管理，并保障订户密钥传输的安全。

6.1.3 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道，经注册机构传递到 SZCA。

订户的加密证书公钥由 KMC 通过安全通道传递到 CA 中心。

从 RA 到 CA 以及从 KMC 到 CA 的传递过程中，采用国家密码管理局许可的通讯协议及密钥算法，保证了传输中数据的安全。

6.1.4 电子认证服务机构公钥传送给依赖方

SZCA 的根公钥包含在 SZCA 自签的根证书中。证书用户可以从 SZCA 的网站上下载 SZCA 根证书。

6.1.5 密钥的长度

SZCA 所使用的密钥对长度支持 RSA1024 位，以及国家密码管理局要求的密钥长度。

6.1.6 公钥参数的生成和质量检查

公钥参数由国家密码管理局许可、SZCA 数字证书签发系统支持的硬件产生。

6.1.7 密钥使用目的

加密密钥对和签名密钥对是构建数字证书的重要组成部分，同时可以完成对敏感数据的加解密和数字签名。

订户的签名密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等，加密密钥对可以用于信息加密和解密。 签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块的标准和控制

SZCA 使用国家密码管理局许可的产品，密码模块的标准符合国家规定的要求。其安全性达到以下要求：

- 接口安全：不执行规定命令以外的任何命令和操作；
- 协议安全：所有命令的任意组合，不能得到私钥的明文；
- 密钥安全：密钥的生成和使用必须在硬件密码设备中完成；
- 物理安全：密码设备具有物理防护措施，任何情况下的拆卸均立即销毁在设备内保存的密钥。

6.2.2 私钥多人控制

SZCA 从技术和制度上保证了敏感的加密操作需要在多个可信角色的共同参与下才能完成。在操作现场，必须由 2 位或以上具备权限的密钥管理人员和操作人员，同时对加密机中的密钥进行操作，任何人无法独立完成操作。

6.2.3 私钥托管

对于 CA 密钥 SZCA 无托管业务；对于订户加密私钥的托管，SZCA 将根据国家相关部门的规定执行。

6.2.4 私钥备份

- CA的私钥保存在防高温、防潮湿及防磁场影响的环境中，对私钥的备份操作必须2人或以上才可完成。
- SZCA每天对CA的私钥进行备份。
- RA的私钥由RA产生，由RA自行备份。
- 订户的签名私钥有订户产生，建议定会自行备份，并对备份的私钥采用口令或其他访问控制机制保护，防止非授权的修改和泄漏。

6.2.5 私钥归档

当 SZCA 的 CA 密钥对到期后，这些密钥对将被归档保存至少 5 年。归档的 CA 密钥对保存在本 CP6.2.1 所述的硬件密模块中，当其保存期满时，SZCA 将按照本 CP6.2.10 所述方法进行安全地销毁。

订户加密密钥的归档由 KMC 负责。

SZCA 不对 RA 和订户签名密钥归档。

6.2.6 私钥导入、导出密码模块

SZCA 的 CA 密钥对在硬件密码模块上生成，保存和使用。此外，为了常规恢复和灾难

恢复，SZCA 对 CA 密钥进行复制。当 CA 密钥对从一个硬件密码模块复制到另一个硬件密码模块上时，被复制的密钥对以加密的形式在模块之间传送，并且在传递前要进行模块间的相互身份鉴别。另外 SZCA 还有严格的密钥管理流程对 CA 密钥对复制进行控制。所有这些有效防止了 CA 私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

6.2.7 私钥在密码模块的存储

私钥在硬件密码模块中加密保存。

6.2.8 激活私钥的方法

具有激活私钥权限的管理员使用含有自己身份的加密 IC 卡登录，启动密钥管理程序，并进行激活私钥的操作，需要 2 名管理员同时在场监督。

6.2.9 解除私钥激活状态的方法

具有解除私钥激活状态权限的管理员使用含有自己身份的加密 IC 卡登录，启动密钥管理程序，并进行解除私钥的操作，需要 2 名管理员同时在场监督。

6.2.10 销毁私钥的方法

具有销毁私钥权限的管理员使用含有自己身份的加密 IC 卡登录，启动密钥管理程序，并进行销毁私钥的操作，需要 3 名管理员同时在场监督。

6.2.11 密码模块的评估

由国家密码管理部门负责。

6.3 密钥对管理的其它方面

6.3.1 公钥归档

对于生命周期外的 CA 和最终订户证书，SZCA 进行归档，归档的证书存放在归档数据库中。

6.3.2 证书操作期和密钥对使用期限

订户证书有效期通常为 1-5 年，订户密钥有效期与其证书有效期相同。

SZCA 根证书有效期为 5 年，CA 密钥有效期与根证书有效期一致。

6.4 激活数据

6.4.1 激活数据的产生和安装

CA 私钥的激活数据，必须按照关于密钥激活数据分割和密钥管理办法的要求，严格进行生成、分发和使用。

订户的激活数据包括下载证书的口令、用户密钥存储介质的 PIN 码等。下载证书的口令由 SZCA 在安全可靠的环境下随机产生，通过可靠的方式发送给订户。证书存储介质（如：E_Key）出厂时设置有缺省 PIN 码，订户使用证书前，需重新进行设置。为保证私钥安全，SZCA 推荐订户使用密码口令。

6.4.2 激活数据的保护

对于 CA 私钥的激活数据，SZCA 将激活数据按照可靠的方式分割后由不同的可信人员保管，并且各保管人必须符合职责分割的要求。

订户的激活数据必须进行妥善的保管，或者记住以后进行销毁，不可被他人所获悉。如果订户证书使用口令或 PIN 码保护私钥，订户应妥善保管好其口令或 PIN 码，防止泄漏或窃取。同时，为了配合业务系统的安全需要，应该经常对激活数据进行修改。

6.4.3 激活数据的其它方面

考虑到安全因素，对于订户激活数据的生命周期，规定如下：

1. 订户用于下载证书的口令，下载成功后失效。

2. 用于保护私钥或者 IC 卡、USB Key 的口令，建议订户根据业务应用的需要随时予以变更，使用期限超过 3 个月后一定要进行修改。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

SZCA 的数字证书签发系统的数据文件和设备由 SZCA 系统管理员维护，未经 SZCA 管理员授权，其它人员不能操作和控制 SZCA 系统；其它普通用户无系统账号和密码。SZCA 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。

SZCA 系统密码有最小密码长度要求，而且必须符合复杂度要求，SZCA 系统管理员定期更改系统密码。

6.5.2 计算机安全评估

SZCA 使用的密码设备是通过国家密码管理局批准生产的密码设备。

6.6 生命周期技术控制

6.6.1 系统开发控制

SZCA 的系统由国家相关的安全标准和具有密码标准资质的可靠开发商开发，其开发过程符合 SZCA 系统管理的各项规定

6.6.2 安全管理控制

SZCA 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 SZCA 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。

6.6.3 生命期的安全控制

SZCA 认证业务系统的软硬件设备具备可持续性的升级能力，其中包括了对软、硬件生命周期的控制，以保证其安全性和可靠性。

6.7 网络的安全控制

SZCA有防火墙以及其它的访问控制机制保护，其配置只允许已授权的机器访问。只有经过授权的SZCA员工才能够进入SZCA签发系统、SZCA注册系统、SZCA目录服务器、SZCA证书发布系统等设备或系统。所有授权用户必须有合法的安全证书，并且通过密码验证。

7.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

颁发者：指定签发机构的DN名，由国家、省、市、组织机构、单位部门和通用名等组成。

CN=SZCA=ShenZhen Digital Certificate Authority Center CO.LTD

L=SHENZHEN

S=GUANGDONG

C=CN

生效时间：此次CRL的生效时间。

下一次的更新时间：下次CRL签发时间。

签名算法：SZCA采用sha1RSA签名算法。

颁发机构密钥标识符（Issuer Unique Identifier）：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。

撤销证书列表：每个证书对应一个唯一的标示符(即它含有已撤销证书的唯一序列号，并不是实际的证书，废除的证书序列号是指要废除的由同一个CA签发的证书的一个唯一标识号，同一机构签发的证书不会有相同的序列号)。列表中的每一项都含有证书不再有效的时间。

CRL发布：SZCA周期性自动发布最新的CRL。。

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

一个OCSP状态请求包括以下域：

- Version：客户端使用OCSP协议的版本号； SZCA在线证书状态协议为v1版。
- Request or Name：为可选项，表示发起请求的实体名（DN）。
- Request List：表示一个请求序列。
- Signature Algorithm：为可选项，标识对本请求信息签名的算法。
- Signature：为可选项，本请求信息的数字签名。
- Certs：为可选项，请求状态的证书序列。

7.3.2 OCSP 响应

当一个确定的 OCSP 的响应消息包含以下域：

- Version：OCSP 响应者使用的 OCSP 协议版本号；SZCA 的在线证书状态协议为 v1 版。
- Responder ID：响应者实体的公钥的消息摘要或者响应者的 DN。
- Produced At：该响应生成的日期和时间；
- Responses：包含对每一个请求的响应序列，每个单独响应包含以下域。
- Response Extensions：为可选项，指明响应中含有的 OCSP 扩展项。
- Signature Algorithm：响应者对该响应消息签名所采用的算法；
- Signature：本响应消息的数字签名。
- Certs：为可选项，包含被请求状态的实际证书的一个序列。

7.3.3 OCSP 扩展项

- Nonce(一次性随机数)：在状态请求消息中的每一个 request Extensions 变量和响应消息中的 Response Extension 变量中包含一次性随机数，防止重放攻击。
- CRL 引用：该扩展项指明一个 CRL，在该 CRL 中可以找到已经撤销或者冻结的证书；
- 可接受的响应类型：指明可以理解的响应类型的对象标识符；
- 服务定位符：该扩展项中通常包含证书颁发者的 DN 和一个 OCSP 服务器定位符。

8.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

信息产业主管部门评估完成后，SZCA 将根据评估的结果检查缺失和不足，提交修改和预防措施以及整改计划书，并接受其对整改计划的审查，以及对整改情况的再次评估。

SZCA 完成内部评估后，评估人员需要列出所有问题项目的详细清单，由评估人员和被

评估对象共同讨论有关问题，并将结果书面通知 SZCA 运营安全管理小组和被评估者，进行后续处理。

SZCA 将根据普遍认可的国际惯例或监管法律迅速解决问题。

8.6 评估结果的传达与发布

SZCA 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，SZCA 将不公开审计或评估结果。SZCA 内部评估结果处分权归 SZCA 所有。任何人未经 SZCA 许可发布或泄漏的审计或评估结果，SZCA 将保留追究其法律责任的权利。

9.法律责任和其他业务条款

9.1 费用

证书相关费用在 SZCA 的网站 https://www.szca.com 上公布。价目表按 SZCA 明确指定的时间生效，若没有指定生效时间的，自价目表公布之日起生效。SZCA 也可以通过其它方法通知订户或其它各方费用变化。具体价格参照广东省物价部门相关文件执行。

如果 SZCA 与订户或 SZCA 关联单位签署的协议中指明的价格和 SZCA 公布的价格不一致，以协议中的价格为准。

9.1.1 证书签发和更新费用

参见 CP9.1。

9.1.2 证书查询费用

对于证书查询，目前 SZCA 暂不收取任何费用。除非用户提出的特殊需求，需要 SZCA 支付额外的费用，SZCA 将与用户协商收取相应的费用。

9.1.3 证书撤销或状态信息的查询费用

对于证书撤销或状态信息的查询，目前 SZCA 暂不收取任何费用。

9.1.4 其它服务费用

参见 CP9.1。

9.1.5 退款策略

在实施证书操作和签发证书的过程中，SZCA 遵守并保持严格的操作程序和退款策略。一旦订户接受数字证书，SZCA 将不办理退证退款手续。除非订户可以通过合法途径证明 SZCA 违背了 CPS 有关订户或订户证书方面所规定的责任或其它重大义务，否则 SZCA 向用户收取的费用均不退还。因为证书撤销等原因确实需要退还预付费用的，订户需要填写退

款申请表，并发送给 SZCA，以要求退款。此退款策略不限制订户得到其它的赔偿。完成退款后，订户如果继续使用证书，SZCA 将追究其法律责任。

9.2 财务责任

9.2.1 保险范围

无

9.2.2 对最终实体的保险和担保

根据《中华人民共和国电子签名法》的规定，订户在此同意：由于 SZCA 的责任给订户造成的直接损失，SZCA 仅赔偿订户一定金额的直接损失，即 SZCA 将根据使用证书的种类，承诺一定额度的赔付具体情况参见本 CP9.8.

9.3 业务信息的保密

9.3.1 保密信息范围

保密信息包括但不限于以下内容：

1.SZCA 与 SZCA 授权的发证机关之间、SZCA 与订户之间、SZCA 授权的发证机构与订户之间、SZCA 与其它证书服务相关方、SZCA 关联方之间的协议、往来函和商务协定等。

2.与证书持有者证书公钥配对的私钥。

3.SZCA 或 SZCA 对发证机构的审计记录、审计报告、审计结果等。

4.有关 SZCA 认证体系的运营信息。

5.灾备计划、应急方案、安全措施等内部流程管制文件。

6.订户证书信息以外的个人隐私信息。

以上信息除非法律明文规定或政府、执法部门等的要求，或 SZCA 认为有必要，SZCA

没有义务也不会对外公布或披露。

9.3.2 非保密信息

1.与证书有关的申请流程、申请需要的手续、申请操作指南、CPS 等。

2.证书持有者证书中包括的相关公开信息。

3.证书状态及撤销列表信息。

4.其他可以通过公共、公开渠道获得的信息。

虽然上述属非保密信息，并不意味着其能够被第三方任意不被授权的使用，SZCA 和信息的所有人保留所有这些信息的知识产权。

其它：SZCA 信息的保密性取决于特殊的数据项和申请。

9.3.3 保护保密信息的责任

SZCA、任何订户、关联体以及与认证业务相关的参与方等，皆有义务按照本 CP 的规定，承担相应的保护保密信息的责任。

当 SZCA 在任何法律、法规或规章条款的要求下，或在法院的要求下披露本 CP 所载具有保密性质的信息时，SZCA 可以按照法律、法规或规章条款以及法院的判定的要求，向执法部门披露相关的保密信息。这种披露视为不违反保密的要求和义务。

当机密信息的所有者要求 SZCA 公开或披露他所拥有的保密信息，SZCA 将在法律法规允许的情况下满足其要求；同时，SZCA 将要求所有者对这种申请进行书面授权，以表示其自身的公开或者披露的意愿。如果这种披露保密信息的行为涉及任何其它方的赔偿义务，SZCA 不承担任何与此相关的或由于公开保密信息所造成的损失。保密信息的所有者应负责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，包括 SZCA 的损失在内。

9.4 个人信息的保密

9.4.1 隐私保密方案

SZCA 尊重所有的用户和他们的隐私，并按照我国信息安全方面的法律法规的要求和国际公认的个人数据隐私保护原则执行，本 CP 将自动予以引用并将之作为隐私保护的基本依据来执行。

任何人选择使用 SZCA 的任何服务，那么就表示已经同意接受 SZCA 有关隐私保护的声明。

9.4.2 作为隐私处理的信息

SZCA 在管理和使用订户申请、注册证书时提供的相关信息时，除了证书已经包括的信息外，该订户的基本信息和身份认证资料，非经订户同意或者法律法规及权力部门的合法要求，绝对不会任意对外公开。

9.4.3 非保密的个人信息

证书订户持有的证书内包括的信息，以及该证书的状态信息等，是可以公开的，将不被视为隐私信息。

9.4.4 保护隐私的责任

SZCA、任何订户、关联体以及与认证业务相关的参与方等，都有义务按照本 CP 的规定，承担相应的保护保密信息的责任。

当 SZCA 在任何法律法规或者法院通过合法程序的要求下，或者信息所有者书面授权的情况下，SZCA 可以向特定对象披露相关的隐私信息。SZCA 无须为此承担任何责任，而且这种披露不被视为违反了隐私保护义务。如果这种隐私披露导致了任何损失，SZCA 对此不应承担任何责任。

9.4.5 使用隐私信息的告知与同意

SZCA 在其认证业务范围内使用所获得的任何订户信息，只用于订户身份识别、管理和服务订户的目的。在使用这些信息时，SZCA 将按照我国现行有效法律的规定，对用户进行告知并获得其授权同意。

SZCA 在任何法律法规规定或者法院通过合法程序的要求下，或者信息所有者书面授权的情况下向特定对象披露隐私信息时，也没有告知订户的义务，并且不需得到订户的同意。

SZCA 与其授权注册机构如果需要将客户隐私信息用于双方约定的用途以外的目的，在法律允许的情况下，事前需告知订户，并得到用户的同意和书面签章授权。

9.4.6 依法律或行政程序的信息披露

除非符合下列条件之一，否则 SZCA 绝对不会将订户的基本注册资料和身份认证信息提供给任何对象，包括法院、政府机构等单位：

- 政府法律法规的规定并且经过主管单位合法的授权程序提出申请
- 法院处理因使用证书产生的纠纷或仲裁时合法的提出申请
- 具有合法司法管辖权的诉讼、仲裁机构的正式申请
- 国家司法机关开具证明需我司配合取证，例：公安、检察院、法院、工商、
- 证书订户以书面方式进行授权

9.4.7 其它信息披露情形

其它信息披露亦需在法律法规和订户协议许可范围内。

9.5 知识产权

SZCA 享有并保留对证书以及 SZCA 提供的全部软件、资料、数据的独占知识产权，包括保证证书和软件的完整权、冠名权、著作权和利益分享权等。因此，SZCA 有权决定关联实体采用的软件系统，选择采取的形式、方法、时间、过程和模型，以便保证系统的兼容和互通。

按本 CP 规定，所有与 SZCA 发行的证书和 SZCA 提供的软件相关的一切版权、商标和其它知识产权均属于 SZCA 所有，这些知识产权包括相关的文件和使用手册。SZCA 授权电子认证服务机构在征得 SZCA 的同意后，可以使用相关的文件和手册，并有责任和义务提出修改意见。

在没有 SZCA 事先书面同意的情况下，任何使用者不能在任何证书到期、作废或终止后，使用或接受任何 SZCA 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。

9.6 陈述与担保

除非 SZCA 在协议中做出特别约定，如果本 CP 的规定与其它 SZCA 制订的相关规定、指导方针相互抵触，用户必须接受本 CP 的约束。在 SZCA 与包括订户在内的其它方签订的仅约束签约双方的协议中，对协议中未约定的内容，视为双方均同意按本 CP 的规定执行；对协议中不同于本 CP 的约定，按双方协议中约定的内容执行。

9.6.1 电子认证服务机构的陈述与担保

SZCA 的一般陈述：

- 建立电子认证业务规则（CPS）和其它认证服务所必需的规范、制度体系。
- 在本CP 相关条款规定的范围内，提供基础设施和认证服务，遵守本CP 的各项规范。
- 建立和执行符合国家相关政策的规定的安全机制以保证SZCA本身的签名私钥得到安全的存放和保护。
- 所有和认证业务相关的活动都符合法律法规和主管部门的规定。
- SZCA及其授权证书服务机构不是证书订户或依赖方的代理人、受托人、管理人或其它代表。SZCA和证书订户的关系以及SZCA和依赖方的关系并不是代理人和委托者的关系。证书订户和依赖方都没有权利以合同形式或其它方法让SZCA承担信托责任。SZCA也不能用明示、暗示或其它方式，做出与上述规定相反的陈述。

SZCA 对订户的陈述:

除非本 CP 中另有规定或者发证机构和订户间另有协议，SZCA 向在证书中所命名的订户承诺：

- 在证书中没有发证机构所知的或源自于发证机构的错误陈述。

- 在生成证书时，不会因发证机构的失误而导致数据转换错误，即不会因发证机构的失误而使证书中的信息与发证机构所收到的信息不一致。
- 发证机构签发给订户的证书符合本CP 的所有实质性要求。
- 发证机构将按本CP的规定，及时撤销或挂起证书。
- 发证机构将将做出合理努力向订户通报任何已知的，将在本质上影响签发给订户的证书的有效性和可靠性的事件。

上述陈述仅仅是为保证订户的利益，而不是用于使任何其它方受益或被其它方强迫执行。发证机构的行为若符合本 CP 和相关法律的规定，既视为发证机构做出了上述描述的合理的努力。

发证机构对依赖方的陈述。

发证机构就其所发证书向所有按照本 CP 合理地信赖签名（该签名可通过证书中所含的公钥验证）的人承诺：

- 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。
- 发证机构完全遵照本CP 的规定签发证书。

SZCA 有关公开发布的陈述

通过公开发布证书，发证机构向 SZCA 信息库和所有合理依赖证书中信息的人证明：发证机构已向订户签发了证书，并且订户已经按照本 CP 中的规定接受了该证书。

9.6.2 注册机构的陈述与担保

注册机构 RA 按照程序取得了 SZCA 的授权后，将保证：

- 遵循本CP和SZCA的授权协议和其它SZCA公布的标准和流程，接受并处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必须遵循SZCA制订的服务受理规范、系统运作规范和管理规范，根据本CP、

SZCA公布的规范，RA有权决定是否为申请者提供相应的证书服务。

- 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存档，涵盖并且不得与SZCA公布的相关条款产生冲突、矛盾或者不一致。

- 依据本CP的规定，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承诺严格执行为所有证书用户提供隐私保密的义务，并愿意承担因此而带来的法律责任。

- 接受SZCA根据本CP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。

- 承认SZCA对所有证书服务申请者的服务请求拥有最终处理权。

- 为证书申请者提供必要的技术咨询，使证书申请者顺利地申请和使用证书。

9.6.3 订户的陈述与担保

一旦接受发证机构签发的证书，自接受之时起直至证书的使用有效期满为止，如果订户不另行通知，那么订户被视为向 SZCA 及所有合理信赖证书中所含信息的人做出如下保证：

- 在证书申请材料上填列的所有声明和信息必须是完整、精确、真实和正确的，可供SZCA检查和核实；并且，愿意承担任何提供虚假、伪造等信息的法律责任

- 如果存在代理人，那么订户和代理人两者负有无限连带责任。订户有责任就代理人所作的任何不实陈述与遗漏，通知SZCA或其下属发证机构

- 用于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，证书是有效证书并已被订户接受（证书没有过期、挂起或撤销）。

- 未经授权的人员从未访问过订户私钥。

- 订户向发证机构陈述的所有包含在证书中的有关信息是真实、完整的。

- 就订户所知道的或注意到的包含在证书中的信息，都是真实的。如果订户发现了

证书中信息存在某些错误，但订户还没有及时通知给发证机构，那么，发证机构认为：订户认为上述信息都是真实的。

- 证书将按本CP 的规定，只用于经过授权的或其它合法的使用目的。

- 除非经订户和发证机构间的书面协议明确批准，订户保证不从事发证机构（或类似机构）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（或认证其它任何形式的公钥）或证书撤销列表。

- 一经接受证书，既表示订户知悉和接受本CP 中的所有条款，并知悉和接受相应的订户协议。

- 一经接受证书，订户就应承当如下责任：即始终保持对其私钥的控制，使用可信的系统，和采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用。

- 一经接受证书，订户即同意使SZCA免于由下列原因直接或间接造成的任何责任和损失：订户（或其授权的代理人）虚假地或错误地陈述了事实；订户未能披露重要事实，而订户的这种有意或无意的错误陈述或失职造成了对SZCA和任何信任其证书的人的欺骗；订户没有使用可信系统或没有采用必要的合理措施防止其私钥被损害、丢失、泄露、被篡改或被未经授权使用。如果因此给SZCA造成任何责任、损失、任何诉讼及一切费用，订户将予以经济赔偿。

- 作为证书申请者，有责任就申请代理人的疏忽和错误陈述及时通知证书签发者。

9.6.4 依赖方的陈述与担保

依赖方在信赖任何 SZCA 签发的证书时，就意味着保证：

- 熟悉本CP的条款以及和所信赖订户证书的证书政策，了解证书的使用目的。

- 依赖方在信赖SZCA签发的证书前，已经对证书进行过合理的检查和审核，包括：检查SZCA公布的最新的CRL，以获得该证书的状态，只有确认该证书没有被撤销时，SZCA才保证该证书是有效的；检查该证书信任路径中所有出现过的证书的可靠性；检查该证书的有效期以及适用范围。

- 一旦由于疏忽或者其它原因违背了合理检查的条款，依赖方愿意就此对SZCA带来

的损失进行补偿，并且承担因此造成的自身或他人的损失。

- 对证书的信赖行为就表明依赖方已经接受本CP的所有规定，尤其是其中有关免责、拒绝和限制义务的条款。

9.6.5 其它参与者的陈述与担保

无规定

9.7 担保免责

除非在本 CP 第 9.6.1 中明确承诺外，SZCA 不承担其它任何形式的保证和义务，同时 SZCA 将：

1. 由于不可抗力因素导致 SZCA 暂停、终止部分或全部数字证书服务，SZCA 不承担赔偿责任。

2. 订户违反本 CP 第 9.6.3 之承诺时，或者证书依赖方违反本 CP 第 9.6.4 之承诺时，得以免除 SZCA 的责任；

3. 不对电子认证活动中使用的任何软件做出保证。

4. 由于非 SZCA 原因造成的软件、硬件故障、网络中断导致证书错报、交易中断或其他是有造成的损失，SZCA 不承担责任。

5.SZCA 只在证书有效期内承担赔偿责任。

6.证书订户或者其它有权提出撤销或挂起证书的人提出撤销或挂起请求后，到 SZCA 实际完成撤销或挂起该证书结束的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果 SZCA 按照本 CP 的规范进行了有关操作，SZCA 不承担任何损害赔偿责任。

7. SZCA 在法律许可的范围内，依据法律、法规等以及受害者的要求如实提供电子政务、电子商务或其他网络作业中不可抵赖的电子签名依据，但并不对此承担法律或法规规定之外的责任。

9.8 有限责任

对于由于 SZCA 自身原因导致当事人损失的（不能通过合法渠道证明的除外），SZCA 将承担相应赔偿责任。但这种责任是有限的。SZCA 只对因信赖证书而产生的直接损害负责，而不负间接损害赔偿、利润利息损失、精神损害、惩罚性赔偿等责任。基于以上赔偿范围，SZCA 及其授权的发证机构，对所有当事人（包括但不限于订户、申请者、接受者或信赖方）的合计赔偿责任，不超过如下所述的对这些证书的赔偿限额。

对于一份特定证书的所有签名和交易业务，SZCA 及其授权的发证机构，对于任何人或任何单位有关该特定证书的合计赔偿金额限制在不超出下述数额的范围内（单位：人民币元）：

1. 个人类证书，不超过 800 元；

2. 单位类证书，不超过 4000 元；

3. 设备类证书，不超过 8000 元。

本条款适用于一定形式的损害，包括但不局限于任何人（包括但不限于订户、证书申请者、接收方或信赖方）由于信任或使用 SZCA 签发、管理、使用、挂起或撤销的证书或已过期证书而导致的直接的、补偿性的、间接的、特别的、结果的、惩戒性的或意外的损害。

本条款也适用于其它责任，如合同责任、民事侵权责任或任何其它形式的责任。每份证书的赔偿责任均有限额，而不考虑数字签名、交易处理或有关的其它索赔的数量。当超过赔偿限额时，除非得到管辖法院的仲裁或判决，可用的赔偿限额将首先分配给在该纠纷中最早得到索赔解决的一方。SZCA 没有责任为每个证书支付高出赔偿限额的赔偿，而不管赔偿限额总和在索赔者之间是如何分配的。

9.9 赔偿

在签发证书时，未按照本 CP 的规定进行操作，或者违反法律法规的要求而造成证书订户损失的；SZCA 承担如 CP9.8 所述有限赔偿责任。

有下列情形之一的，订户或依赖方应承担相应的损失赔偿责任：

- 订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致造成SZCA、注册机构或者第三者遭受损害的。
- 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SZCA，以及不当交付他人使用造成SZCA、第三方遭受损害的。
- 订户使用证书或者依赖方信任订户证书，有违反本CP及相关操作规范，或者将证书用于非本CP规定的其它业务范围的。
- 用户使用或信赖证书时，未能依照本CP等规范进行合理审核，导致SZCA或第三方遭受损害的。
- 证书订户或者其它有权提出撤销或挂起证书的人提出撤销或挂起请求后，到SZCA实际完成撤销或挂起该证书结束的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果SZCA按照本CP的规范进行了有关操作，那么该证书订户必须承担所有损害赔偿责任。
- SZCA与之签署的协议另有赔偿规定的，从其规定。

9.10 有效期和终止

9.10.1 有效期限

本 CP 自发布之日起正式生效，文档中将详细注明版本号及发布日期，最新版本请访问 SZCA 网站以获得，对具体个人不做另行通知，当新版本正式发布生效，旧版本将自动终止。

9.10.2 终止

本 CP 及其更新版本在 SZCA 终止电子认证服务时失效。在终止服务六十日前向信息产业主管部门报告，并做出妥善安排。

9.10.3 效力的终止与保留

在本 CP 中涉及审计、保密信息、隐私保护、归档、知识产权的条款，以及涉及 SZCA 赔偿责任及有限责任的条款，在本 CP 终止后仍然继续有效存在。

9.11 对参与者的个别通告与沟通

SZCA 及其授权注册机构在必要的情况下，如在提前终止 CP 时，会通过适当方式，如电话、电子邮件、信函、传真等，个别通知订户、依赖方。

9.12 修订

9.12.1 修订程序

SZCA 将尽量避免对本 CP 进行不必要的修改。然而 SZCA 将不定期地对本 CP 进行审查、评估，确保其符合国家法律法规和主管部门的要求，符合认证业务开展的实际需要。

此处所提及修订分为重大修订和非重大修订，大体上，重大修订主要指各参与方权责的改变等重要的修订，非重大修订是指如联系方式的改变等不重要的修订。SZCA 在区分重大修订和非重大修订时有酌情权。

具体修订程序详见本 CP1.5.4“CP 批准程序”。

9.12.2 通知机制和期限

SZCA 有权在合适的时间修订和改变 CP 中任何术语、条件和条款，而且无须预先通知任何一方。

SZCA 在网站 https://www.szca.com 信息库中设置和公布修订结果。如果关于 SZCACP 的修改被放置在 SZCA 信息库中的规范更新和通知栏(查看 https://www.szca.com)，它对于修改 SZCACP 同样有效。这些修改将取代 CP 原有版本中的任何冲突和指定条款。

所有以书面形式提供给订户的 CP 修订，按以下规则发送：

- 接受者是公司或其它单位组织向其登记联系地址或办公室发送信息。
- 接受者是个人向其申请书上规定地址发送。
- 这些通知可能用快递或挂号信的方式发送。
- SZCA可以选择通过电子邮件或其它方式向订户发送通知，邮件地址在订户申请证

书时已注明。

9.12.3 修订同意

对于非重大修订，无需经各参与方同意，修订后 CP 将在发布之时即生效。

对于重大修订，在修订的 CP 发布后的 15 天内，证书申请者和订户没有请求撤销其证书，将被视为同意该修订，所有的修订和改变立刻生效。

9.12.4 必须修改业务规则的情形

如果出现下列情况，那么必须对 CP 进行修订，对 CP 的必要修订将在发布 15 天以后生效。除非在这 15 天结束前，SZCA 以同样的方式发表一个撤消修订的通知。

- 密码技术出现重大发展，足以影响现有CP的有效性
- 有关认证业务的相关标准进行更新
- 认证系统和有关管理规范发生重大升级或改变
- 法律法规和主管部门的要求
- 现有CP出现重要缺陷
- 应用出现新的要求

9.13 争议处理

作为证书认证争议裁决的专家机构，SZCA 运营安全管理小组专家组收集相关的证据以促进争议解决，协调 SZCA 服务体系、当事人之间的相互关系，并作为争议建议报告的最终撰写人。无论专家组是否完成建议报告并将建议传达，以及形成怎样的裁决决定，并不妨碍 SZCA、当事人及其它关联利益方采取与管辖法律和本 CP 一致的方式，寻找其它的解决措施。

除非争议中的当事人书面一致同意选择争议解决机制（比如仲裁），否则就执行 SZCACP 及 SZCA 与任何一方签订的协议中提起的诉讼或有关当事人之间的相关的商业关系引起的诉讼都将提交到 SZCA 工商注册所在地的人民法院。各方在此同意将争议案件提交 SZCA

工商注册所在地的人民法院。

9.14 管辖法律

本电子认证业务规则接受《中华人民共和国电子签名法》、《电子认证服务管理办法》以及其它中华人民共和国法律的管辖和解释。

无论合同或其它法律条款的选择及无论是否在中国建立商业关系，SZCACP 的执行、解释、翻译和有效性均适用中华人民共和国的法律。法律的选择是确保对所有订户有统一的程序和解释，而不管他们在何地居住以及在何处使用证书。

9.15 与适用的法律的符合性

SZCA 的各项策略均遵守并符合中华人民共和国各项法律法规和国家信息主管部门的要求。若本 CP 所涉及条款被主管部门宣布为非法、不可执行或无效时 SZCA 将对该不符合性条款进行修订，直至该条款合法并可执行为止。本 CP 某一条款的无效，不影响其余条款的法律效力。

9.16 一般条款

9.16.1 完整协议

本 CP 将替代先前的与主题相关的书面或口头解释，并与订户协议、依赖方协议及补充协议构成 SZCA 与各方参与者之间的完整协议。

9.16.2 转让

若 SZCA 因不可抗力或其他原因停止电子认证服务，SZCA 之所属订户需按国家规定接受相应接管 CA 的证书服务条款。

除以上原因外，SZCA、订户及依赖方之间的责任和义务不得以任何形式转让。

9.16.3 分割性

本 CP 的任何条款或其应用，如果因为某种原因或在任何范围内发现无效或不能执行，那么 CP 其余的部分仍然有效。相关当事人了解并同意，SZCACP 所规定的责任限制、保证或其它免责条款或限制、或损害赔偿的排除等，均可独立于其它条款的个别条款，并可加以执行。

9.16.4 强制执行

无

9.16.5 不可抗力

本 CP 提及的不可抗力是指“不能预见、不能避免和不能克服的客观情况”。

不可抗力主要包括但不限于以下几种情形：

（1）自然灾害、如台风、洪水、冰雹；

（2）政府行为，如征收、征用；

（3）社会异常事件，如罢工、骚乱。

（4）互联网或其他基础设施无法使用。

9.17 其它条款

SZCA 对本 CP 拥有最终解释权。