深圳 CA 全球信任体系

电子认证业务规则

深圳市电子商务安全证书管理有限公司

二零二零年

深圳 CA 全球信任体系

电子认证业务规则

Shenzhen CA Global Trust Certification Practices Statement

(深圳 CA CPS)

版本V1.0

2020年

https://www.szca.com

版本控制表

文档名称	深圳 CA 全球信任体系电子认证业务规则	保密级别	公开
版本历史变更信息			
版本	生效时间	发布者	备注
V1.0	2020 年	深圳 CA	

版权声明

目录

1. 概括性描述 1

1.1 概述 1

1.2 文档名称与标识 4

1.3 电子认证活动参与者 4

1.3.1 电子认证服务机构 4

1.3.2 注册机构 4

1.3.3 订户 5

1.3.4 依赖方 5

1.3.5 其他参与者 5

1.4 证书应用 5

1.4.1 适合的证书应用 5

1.4.2 限制及禁止的证书应用 6

1.5 策略管理 6

1.5.1 策略文档管理机构 6

1.5.2 联系人 6

1.5.3 决定 CPS 符合策略的机构 7

1.5.4 CPS 批准程序 7

1.6 定义和缩写 7

2. 信息发布与信息管理 12

2.1 信息库 12

2.2 认证信息的发布 12
2.3 发布的时间或频率 12
2.4 信息库访问控制 13
3. 身份标识与鉴别 14
3.1 命名 14
3.1.1 名称类型 14
3.1.2 对名称意义化的要求 14
3.1.3 订户的匿名或伪名 14
3.1.4 理解不同名称形式的规则 14
3.1.5 名称的唯一性 15
3.1.6 商标的识别、鉴别和角色 15
3.2 初始身份确认 15
3.2.1 证明拥有私钥的方法 15
3.2.2 组织机构身份的鉴别 15
3.2.3 个人身份的鉴别 18
3.2.4 没有验证的订户信息 18
3.2.5 授权确认 18
3.2.6 互操作准则 19
3.3 密钥更新请求的标识与鉴别 19
3.3.1 常规密钥更新的标识与鉴别 19
3.3.2 吊销后密钥更新的标识与鉴别 19

3.4 吊销请求的标识与鉴别 20

4. 证书生命周期操作要求 21

4.1 证书申请 21

4.1.1 证书申请实体 21

4.1.2 注册过程与责任 21

4.2 证书申请处理 21

4.2.1 执行识别与鉴别功能 21

4.2.2 证书申请批准和拒绝 22

4.2.3 处理证书申请的时间 23

4.3 证书签发 23

4.3.1 证书签发中注册机构和电子认证服务机构的行为 23

4.3.2 电子认证服务机构和注册机构对订户的通告 23

4.4 证书接受 23

4.4.1 构成接受证书的行为 23

4.4.2 电子认证服务机构对证书的发布 24

4.4.3 电子认证服务机构对其他实体的通告 24

4.5 密钥对和证书的使用 24

4.5.1 订户私钥和证书的使用 24

4.5.2 信赖方公钥和证书的使用 24

4.6 证书更新 25

4.6.1 证书更新的情形 25

4.6.2 请求证书更新的实体 25
4.6.3 证书更新请求的处理 25
4.6.4 颁发新证书时对订户的通告 26
4.6.5 构成接受更新证书的行为 26
4.6.6 电子认证服务机构对更新证书的发布 26
4.6.7 电子认证服务机构对其他实体的通告 26
4.7 证书密钥更新 26
4.7.1 证书密钥更新的情形 26
4.7.2 请求证书公钥更新的实体 26
4.7.3 证书密钥更新请求处理 26
4.7.4 颁发新证书时对订户的通告 27
4.7.5 构成接受密钥更新的行为 27
4.7.6 电子认证服务机构对密钥更新证书的发布 27
4.7.7 电子认证服务机构对其他实体的通告 27
4.8 证书变更 27
4.8.1 证书变更的情形 27
4.8.2 请求证书变更的实体 28
4.8.3 证书变更请求的处理 28
4.8.4 颁发新证书时对订户的通告 28
4.8.5 构成接受变更证书的行为 28
4.8.6 电子认证服务机构对变更证书的发布 28

4.8.7 电子认证服务机构对其他实体的通告 28
4.9 证书吊销 28
4.9.1 证书吊销的情形 28
4.9.2 请求证书吊销的实体 30
4.9.3 请求吊销的流程 30
4.9.4 吊销请求宽限期 30
4.9.5 电子认证服务机构处理吊销请求的时限 31
4.9.6 依赖方检查证书吊销的要求 31
4.9.7 CRL 发布频率 31
4.9.8 CRL 发布的最大滞后时间 31
4.9.9 在线状态查询的可用性 31
4.9.10 在线状态查询要求 32
4.9.11 吊销信息的其他发布形式 32
4.9.12 密钥损害的特别要求 32
4.9.13 证书挂起的情形 32
4.9.14 请求证书挂起的实体 32
4.9.15 请求挂起的流程 33
4.9.16 证书挂起的时限 33
4.10 证书状态服务 33
4.10.1 操作特征 33
4.10.2 服务可用性 33

4.10.3 可选特征 33
4.11 订购结束 33
4.12 密钥托管与恢复 34
4.12.1 密钥托管和恢复的策略及行为 34
4.12.2 会话密钥的封装和恢复的策略与行为 34
5.认证机构设施、管理和操作控制 35
5.1 物理控制 35
5.1.1 场地位置与建筑 35
5.1.2 物理访问 36
5.1.3 电力与空调 37
5.1.4 水患防治 37
5.1.5 火灾防护 37
5.1.6 介质存储 37
5.1.7 废物处理 38
5.1.8 异地备份 38
5.2 程序控制 38
5.2.1 可信角色 38
5.2.2 每项任务需要的人数 38
5.2.3 每个角色的识别与鉴定 39
5.2.4 需要职责分割的角色 40
5.3 人员控制 40

5.3.1 资质、经历和无过失要求 40
5.3.2 背景调查程序 41
5.3.3 培训要求 42
5.3.4 再培训周期和要求 43
5.3.5 工作岗位轮换周期和顺序 43
5.3.6 未授权行为的处罚 43
5.3.7 独立合约人的要求 43
5.3.8 提供给员工的文档 43
5.4 审计日志程序 44
5.4.1 记录事件的类型 44
5.4.2 处理日志的周期 45
5.4.3 审计日志的保存期限 45
5.4.4 审计日志的保护 45
5.4.5 审计日志备份程序 45
5.4.6 审计收集系统 46
5.4.7 对导致事件实体的通告 46
5.4.8 脆弱性评估 46
5.5 记录归档 47
5.5.1 归档记录的类型 47
5.5.2 归档记录的保存期限 47
5.5.3 归档文件的保护 48

5.5.4 归档文件的备份程序 48
5.5.5 记录时间戳的要求 48
5.5.6 归档收集系统 48
5.5.7 获得和检验归档信息的程序 48
5.6 电子认证服务机构密钥更替 48
5.7 损害与灾难恢复 49
5.7.1 事故或损害处理程序 49
5.7.2 计算机资源、软件或数据的损坏 50
5.7.3 实体私钥损害处理程序 50
5.7.4 灾害后的业务连续性能力 51
5.8 电子认证服务机构或注册机构的终止 51
6.认证系统技术安全控制 53
6.1 密钥对的生成与安装 53
6.1.1 密钥对的生成 53
6.1.2 私钥传送给订户 53
6.1.3 公钥传送给证书签发机构 53
6.1.4 电子认证服务机构公钥传送给依赖方 54
6.1.5 密钥的长度 54
6.1.6 公钥参数的生成与质量检查 54
6.1.7 密钥使用目的 54
6.2 私钥保护与密码模块工程控制 55

6.2.1 密码模块标准与控制 55
6.2.2 私钥多人控制 55
6.2.3 私钥托管 55
6.2.4 私钥备份 55
6.2.5 私钥归档 56
6.2.6 私钥导入、导出密码模块 56
6.2.7 私钥存储于密码模块 56
6.2.8 激活私钥的方法 56
6.2.9 解除私钥激活状态的方法 57
6.2.10 销毁私钥的方法 57
6.2.11 密码模块的评估 58
6.3 密钥对管理的其他方面 58
6.3.1 公钥归档 58
6.3.2 证书与密钥对使用的有效期 58
6.4 激活数据 58
6.4.1 激活数据的产生与安装 58
6.4.2 激活数据的保护 59
6.4.3 激活数据的其它方面 60
6.5 计算机安全控制 60
6.5.1 特别的计算机安全技术要求 60
6.5.2 计算机安全评估 61

6.6 生命周期技术控制 61
6.6.1 系统开发控制 61
6.6.2 安全管理控制 62
6.6.3 生命期的安全控制 62
6.7 网络安全控制 62
6.8 时间戳 63
7. 证书、证书吊销列表和在线证书状态协议 64
7.1 证书 64
7.1.1 版本号 64
7.1.2 证书扩展项 64
7.1.3 算法对象标识符 66
7.1.4 名称形式 66
7.1.5 名称限制 67
7.1.6 证书策略对象标识符 67
7.1.7 策略限制扩展项的用法 67
7.1.8 策略限定符的语法和语义 67
7.1.9 关键证书策略扩展项的处理规则 67
7.2 证书吊销列表 67
7.2.1 版本 67
7.2.2 CRL 项与 CRL 条目扩展项 67
7.3 在线证书状态协议 68

7.3.1 OCSP 请求和响应处理 69
8.认证机构审计与其它评估 71
8.1 评估的频率或情形 71
8.2 评估者的资质 72
8.3 评估者与被评估者的关系 72
8.4 评估内容 72
8.5 对问题与不足采取的措施 73
8.6 评估结果的传达与发布 73
9. 法律责任和其它业务条款 75
9.1 费用 75
9.1.1 证书签发与更新费用 75
9.1.2 证书查询费用 75
9.1.3 证书状态信息查询费用 75
9.1.4 其它服务费用 75
9.1.5 退款策略 75
9.2 财务责任 76
9.2.1 保险范围 76
9.2.2 其他资产 76
9.2.3 对最终实体的保险与担保 76
9.3 业务信息保密 76
9.3.1 保密信息范围 76

9.3.2 非保密信息 77
9.3.3 保护保密信息的责任 77
9.4 个人信息保密 78
9.4.1 隐私保护方案 78
9.4.2 作为隐私处理的信息 78
9.4.3 非隐私的信息 78
9.4.4 保护隐私的责任 79
9.4.5 使用隐私信息的告知与同意 79
9.4.6 依司法或行政程序进行信息披露 79
9.4.7 其他信息披露情形 80
9.5 知识产权 80
9.6 陈述与担保 81
9.6.1 电子认证服务机构的陈述与担保 81
9.6.2 注册机构的陈述与担保 84
9.6.3 订户的陈述与担保 85
9.6.4 依赖方的陈述与担保 87
9.6.5 其它参与方的陈述与担保 88
9.7 担保免责 88
9.8 有限责任 89
9.9 赔偿 90
9.10 有效期与终止 92

9.10.1 有效期限 92
9.10.2 终止 92
9.10.3 效力的终止与保留 92
9.11 对参与者的个别通告与沟通 92
9.12 修订 93
9.12.1 修订程序 93
9.12.2 通知机制与期限 93
9.12.3 业务规则必需修改的情形 93
9.13 争议处理 94
9.14 管辖法律 94
9.15 与适用法律的符合性 95
9.16 一般条款 95
9.16.1 完整协议 95
9.16.2 转让 95
9.16.3 分割性 95
9.16.4 强制执行 96
9.16.5 不可抗力 96
9.17 其它条款 96

1. 概括性描述

1.1 概述

深圳CA，全称深圳市电子商务安全证书管理有限公司（Shenzhen Certificate Authority Co,.Ltd，英文简称 “SZCA”），成立于2000年8月。深圳CA于2006年8月通过审查获得国家密码管理局颁发的《电子认证服务使用密码许可证》，并于2007年10月获得原信息产业部颁发的《电子认证服务许可证》；且于2010年11月通过国家密码管理局电子政务电子认证服务能力评估，2012年通过卫生部的审核，分别取得电子政务、卫生系统电子认证服务资质。且上述服务资质均处于有效期内。

本文件为《SZCA全球信任体系电子认证业务规则》（SZCA Global Trust Certificate Certification Practice Statement，以下简称“本CPS”），是包括SZCA及其分公司、子公司、注册机构、受理点、及其他授权的服务代理人在内的所有CA体系成员的运营基础，全面阐述SZCA在提供电子认证服务过程中所遵循的规范及准则，及电子认证服务相关参与者所承担的责任，是对于SZCA证书服务活动业务、技术、权利义务方面的声明和描述。

本CPS遵照 CA/B论坛公布的最新版本的《Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates》（中文《公开可信证书签发管理要求》）、《Baseline-Requirements-for-the-Issuance-and-Management-of-Code-Signing-Certificates》（《代码签名证书签发和管理要求》》、《Guidelines For The Issuance And Management Of Extended Validation Certificates》（《EV证书签发和管理指南》）、《Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates》、（《EV代码签名证书签发和管理指南》）等规范及web trust审计认证标准。

本CPS 不仅严格约束SZCA的业务经营活动，并同样适用于订户、依赖方、及其他电子认证活动参与方。所有电子认证活动的参与方，都必须完整地理解和执行本CPS规定的条款，

据此行使权利和承担义务。

SZCA的证书结构体系：

1.RSA证书体系

SZCA ROOT CA 证书的密码算法为RSA，根密钥长度为 4096 bits，下设8个中级 CA 证书，其中：

（1）SZCA EV SL CA ，密钥长度为 4096 bits，签发密钥长度为RSA 2048 bits、3072 bits 、4096 bits的EV SL服务器类证书；

（2）SZCA OV SL CA ，密钥长度为 4096 bits，签发密钥长度为RSA 2048 bits、3072 bits 、4096 bits的OV SL服务器类证书；

（3）SZCA DV SL CA ，密钥长度为 4096 bits，签发密钥长度为RSA 2048 bits、3072 bits 、4096 bits的DV SL服务器类证书；

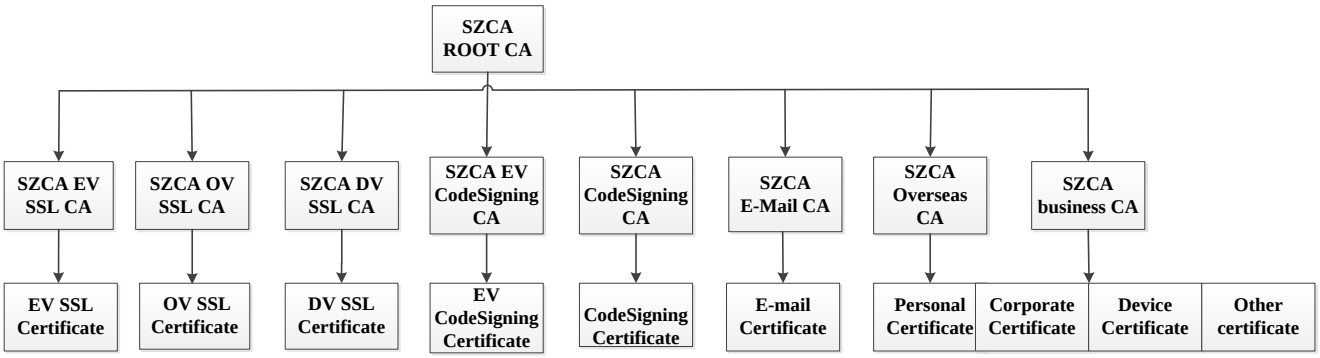
（4）SZCA EV CodeSigning CA ，密钥长度为 4096 bits，签发密钥长度为RSA 3072 bits、4096 bits的EV代码签名证书；

（5）SZCA CodeSigning CA ，密钥长度为 4096 bits，签发密钥长度为RSA 3072 bits、4096 bits的代码签名证书；

（6）SZCA E-Mail CA ，密钥长度为 4096 bits，签发密钥长度为RSA 2048 bits、3072 bits 、4096 bits的电子邮件类证书；

（7）SZCA Overseas CA ，密钥长度为 4096 bits，签发密钥长度为RSA 2048 bits、3072 bits、4096 bits的跨境个人证书、跨境机构证书、跨境设备证书；

（8）SZCA Busines CA ，密钥长度为 4096 bits，签发密钥长度为RSA 2048 bits、3072 bits 、4096 bits的业务个人证书、业务机构证书、业务设备证书。



2. SM2证书体系

SZCA根证书为SZCA SM2 ROOT CA,证书密钥算法为SM2,下含以下6个中级根证书：

（1）SZCA SM2 EV SSL CA，签发SM2算法的EV SSL服务器类证书；

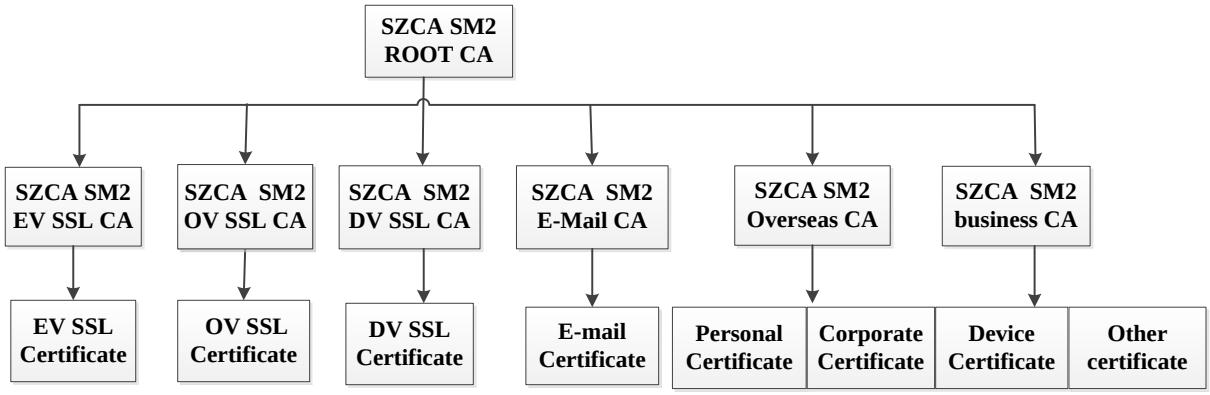
（2）SZCA SM2 OV SSL CA，签发SM2算法的OV SSL服务器类证书；

（3）SZCA SM2 DV SSL CA，签发SM2算法的DV SSL服务器类证书；

（4）SZCA SM2 E-mail CA，签发SM2算法的电子邮件类证书；

（5）SZCA SM2 Overseas CA，签发SM2算法的跨境个人证书、跨境机构证书、跨境设备证书；

（6）SZCA SM2 business CA，签发SM2算法的业务个人证书、业务机构证书、业务设备证书。



1.2 文档名称与标识

本 CPS 名称为《深圳 CA 全球信任体系电子认证业务规则》，又称《SZCA 全球信任体系电子认证业务规则》，对应英文名缩写为 *SZCA Global Trust CPS*，其他类似的指称，也均为本文档名称。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

SZCA，作为合法第三方电子认证服务机构，负责证书签发、更新、吊销、变更等证书管理，密钥管理，提供证书查询、证书黑名单（又称证书吊销列表或CRL）发布、证书策略制定等工作。

SZCA通过数字证书，保障传输、交换的信息的安全性、机密性、完整性、未篡改性，并结合证书的身份认证基础，确保证书使用相关行为的抗抵赖性、防否认性。

1.3.2 注册机构

SZCA的注册机构（Registration Authority,简称“RA”）负责订户证书的申请受理、审核（包括身份标识与鉴别）和管理，不是CA，故不能签署或颁发证书。RA当用于描述、

指称CA机构的职能或角色时，并不一定是独立的机构，可为CA机构的组成部分。

RA在处理SZCA的证书业务时，应遵照电子认证相关法律，并依照本CPS、SZCA的RA相关管理规范及RA业务运营规范，合法开展各类证书申请的受理、身份审核、证书发放等业务。

1.3.3 订户

订户是指向 SZCA 申请证书的实体，其接受、持有并使用证书，为证书的使用行为承担民事责任，通常为自然人、法人或非法人组织（亦称其他组织）。

订户申请数字证书，需阅读、接受本CPS或证书类型对应的CPS，向SZCA提交必要的申请材料，包括合法有效的身份证明材料、签署的电子认证服务协议，缴纳支付认证服务费用。

1.3.4 依赖方

依赖方是指信赖于证书、或其电子签名等所证明的相关事实（包括身份和信息数据）、行为的真实性，并依此进行业务活动的实体。依赖方既可以是订户、也可以不是订户。

1.3.5 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 的数字证书可应用于网络活动中确认主体身份，保障信息加密传输，在电子商务、电子政务、企业信息化、公共服务及知产等领域均有应用。

1.4.2 限制及禁止的证书应用

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;

全球信任体系下的证书根据其类型在功能上有所限制，比如EV SSL服务器证书只能用于经过严格认证的 WEB服务器。

各类证书的密钥用法在订户中扩展项进行了限制。然而基于扩展项限制的有效性取决于应用软件，如果参与方不遵守相关约定其对证书的应用超出本 CPS 限定的应用范围，将不受 SZCA的保护。

(3)任何违反国家法律、法规或破坏国家安全的情形。

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。

用户不应在以上限制、禁止的范围使用证书,否则由此造成的法律后果由订户自行承担。

1.5 策略管理

1.5.1 策略文档管理机构

根据相关法律规定，SZCA指定“SZCA-CPS策略发展小组”负责CPS的起草、注册、维护和更新。“SZCA-CPS策略发展小组”由公司法务人员和技术人员组成，负责本CPS的日常管理及维护工作，包括一般性修订及负责有关本CPS及相关文件的疑问咨询工作。

1.5.2 联系人

任何有关 CPS 的问题、建议、疑问等，请与“SZCA-CPS 策略发展小组”联系：

部门：深圳市电子商务安全证书管理有限公司 SZCA-CPS 策略发展小组

电话：0755-26588399

传真：0755-8615 6366

电子邮件：cps@szca.com

邮寄地址：深圳市南山区高新中二道深圳软件园 8 栋 301 室[518057]。

1.5.3 决定 CPS 符合策略的机构

“SZCA运营安全管理小组”是审批CPS（包含所有版本所有类型的CPS）、决定CPS是否符合对应证书策略的最高决策机构；由SZCA高级管理人员，核心技术人员和法律顾问组成。

1.5.4 CPS 批准程序

“SZCA-CPS策略发展小组”负责起草和修订CPS形成讨论稿（或CPS修订内容），并征求各部门负责人意见，经讨论修改达成一致意见后形成送审稿，并确定文本格式和版本号形成定稿。

“SZCA-CPS策略发展小组”负责将定稿提交“SZCA运营安全管理小组”审阅。经该小组审议通过后，方可对外发布CPS。发布形式应符合行业标准，发布形式包括但不限于网上公布和向客户或合作对象书面提交。发布工作由“SZCA-CPS策略发展小组”协调相关部门完成，并将“SZCA运营安全管理小组”审批意见及CPS电子版存档。本CPS每年至少修订、更新一次，并按上述程序报送审批、备案并发布实施。

自发布之日起，各种形式提供的CPS必须与网站上CPS保持一致，“SZCA-CPS策略发展小组”负责依法在CPS公布之日起三十日内向工业和信息化部备案。

1.6 定义和缩写

表1.1-定义与缩写

缩写/名词	定义
电子认证服务机构	Certificate Authority或Certification Authority， 简称CA，职责是认证身份、签发公钥证书、管理证书密钥的第三方机构。 SZCA及子CA即属于电子认证服务机构。
注册机构	Registration Authority, 简称 RA。RA面向订户，接受订户申请材料、审核订户材料，在订户的CA机构之间传递证书申请、审批及管理信息。
本地注册机构/本地受理点	Local Registration Authority，简称LRA。 CA设立的证书申请受理点，处理证书签发、更新、吊销等申请，其任务是标识与鉴别证书申请者身份，审核申请信息，并批准或拒绝订户证书申请。
电子签名认证证书	可证实电子签名人与电子签名制作数据有联系的数据电文或者其他电子记录。
数字证书	经CA数字签名包含数字证书使用者身份公开信息和公开密钥的电子文件。
订户	申请签发证书，并从CA处接受证书，持有、保管证书或使用证书的实体，包括自然人、法人或其他非法人组织等。
电子签名人	持有电子签名制作数据,并以本人身份或者以其所代表的人的名义实施电子签名的人
依赖方	依赖方（Relying Party），指信赖于证书、电子签名等所证明的相关事实（包括身份和信息数据）、行为、事件的真实性，并依此进行业务活动的实体；或基于对电子签名认证证书或者电子签名的信赖从事有关活动的人
电子认证业务规则/CPS	Certification Practice Statement ，简称CPS，关于CA机构对证书、密钥等的全生命周期的管理活动的详细操作规范和业务操作实践的声明，囊括认证技术、法律责任、认证业务等多方面的内容。
证书吊销（作	Certificate Revocation List ，简称CRL，又称数字证书黑名单。

废）列表/CRL	经CA签名的在证书有效期届满前被吊销而失效、不再受CA机构信任的证书的列表。 CRL包含失效证书的序列号、发布证书的CA机构的名称、发布时间、下次CRL预发行时间。 CA机构周期性发布CRL，供订户或依赖方查询证书有效性使用。
在线证书状态协议/OCSP	Online Certificate Status Protocol ，简称OCSP，供实时查询、检查数字证书的状态信息。
LDAP	Lightweight Directory Access Protocol ，简称LDAP，即轻量级目录访问协议，用于查询、下载数字证书及数字证书吊销列表（CRL）。
电子签名	数据电文中所附或所含的可识别签名者身份，并表明签名者对所签数据及签名数据本身的认可的数据。 数字证书中的电子签名，指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、认证签名者身份及防止其抵赖否认的具有法律效力的数据。
电子签名制作数据	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。 数字证书中的私钥，即是经由数字运算产生的密钥，用于制作电子签名的数据，或就相对应的公开密钥加密的文件或信息予以解密。
电子签名验证数据	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。 数字证书中电子签名验证数据表现为公钥。公钥是经由数字运算产生的密钥，用于验证电子签名，确认电子签名人的身份及电子签名的真实性；或加密数据。
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。包含一对密钥对：私有密钥和公开密钥。
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。包含一对密钥对：私有密钥和公开密钥

SZCA	深圳市电子商务安全证书管理有限公司（Shenzhen Certificate Authority）
CPS策略发展小组	由SZCA任命的负责CPS的编制、修订、日常维护管理与咨询的组织。
SZCA运营安全管理小组	由SZCA任命的负责SZCA的CPS/CP核准及监督其执行的组织。
SZCA超级管理员	负责实施 CA的CP、设置或添加CA管理员、验证审计记录、管理CPS执行的角色、岗位。
SZCA系统管理员	负责安装、配置和维护CA系统的软硬件系统，及 CA服务器的启动和中止的角色、岗位。
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	为证书申请者签发、管理数字证书的软件系统。
SZCA审计员	CA审计员（Auditor）负责 CA系统的证书统计、系统审计。
SSL证书	Secure socket layer certificate，又称域名证书、服务器证书，是通过确认申请人对域名的所有权及控制权，或认证该申请人的身份签发的证书，用以保障网站的真实性，在用户浏览器与服务器端建立安全的通信通道，或防止网站假冒、中间攻击等
代码签名证书	对代码开发、编写、发布人的身份进行认证后签发的证书，申请人用于对代码进行签名，保障代码的完整性、真实性。
注册机构协议	关于SZCA授权的第三方机构担任RA的书面协议，包含授权范围、期限、事项，及履行RA职责与功能的规范、责任义务等条款。
参考码	SZCA为证书申请者颁发证书时生成的，能唯一标识证书申请的字符组合；与授权码相对应。
授权码	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。
证书口令	证书口令指证书中私钥的保护口令。
证书序列号	唯一标识证书的一串字符。
甄别名	Distinguished Name，简称 DN，用于唯一标识订户的名称，该名称需体现订户真实身份、具有实际意义的合法的名称。
密钥管理中心	简称 KMC，负责加密密钥的产生、存储、归档等工作。
PKI	公钥基础设施（Public Key Infrastructure）。
PKCS	公钥密码算法标准（Public Key Cryptography Standard）。

2. 信息发布与信息管理

2.1 信息库

SZCA 信息库是对外公开的信息库，主要面向订户及证书应用依赖方提供信息服务。SZCA 信息库包括但不限于以下内容：证书、 CRL、 CPS、 CP、证书服务协议、技术支持手册、SZCA网站信息以及SZCA不定期发布的信息。

2.2 认证信息的发布

SZCA 的 CPS、CP 以及相关的技术支持信息等在SZCA网站上发布。用户证书可通过SZCA网站查询或下载证书。已被吊销的证书的信息可从 CRL查获；证书的实时状态信息（有效、吊销）可通过 OCSP服务获得。

2.3 发布的时间或频率

编制、修订的CPS，在完成本CPS 1.5.4 所述的批准流程后5个工作日内发布到SZCA的网站，并确保7*24小时可访问。CPS一经发布，即对SZCA、及订户、依赖方产生约束力。修订后生效实施的CPS，如订户未在规定的期间提出异议、或申请吊销证书；对CPS生效前签发的仍处于有效期的证书的订户，同样具有法律效力。

证书签发完成且经订户接受后，SZCA征得用户同意后，于24小时内在本机构的信息库、或其它由订户指定的信息库位置中发布该证书，及定期更新该证书的相关信息。所有被吊销的证书，其CRL通过SZCA的官网下载，更新周期为24小时。CRL的有效期为72小时；特殊情况时，也可人工发布最新CRL。

订户和依赖方可以通过SZCA的官方网站、信息库指定位置查询或获取证书及CRL信息。根据需要，SZCA可提供证书及CRL实时通知服务。

至于其他需要通过信息库向公众公布的信息，其公布内容和公布时间与频次等规则由

SZCA自行决定，但SZCA的信息发布将遵循国家法律法规的规定，并保证发布信息行为是即时、高效的。

2.4 信息库访问控制

SZCA通过信息访问控制机制和安全审计措施，保证只有经过授权的SZCA工作人员才能编写、修改和发布SZCA信息库中的信息。并且授权操作的操作日志、记录将留存并进行审计。SZCA在必要时可自主对信息进行权限管理。但一般而言，对于SZCA的CP、CPS、证书、CRL、技术支持手册等，证书订户及依赖方进行查阅访问不受任何限制。

3. 身份标识与鉴别

3.1 命名

3.1.1 名称类型

SZCA颁发的证书，采用的是X.509 V3标准。证书包含证书颁发机构SZCA和订户主体甄别名（Distinguished Name，简称DN）。

SSL证书的主题别名项应为订户所拥有或控制的域名、IP地址，而DN项的通用名则为主题别名所含若干域名或IP地址的其中之一；另外EV SSL证书主题别名和通用名只能为域名，且不能含通配符。

3.1.2 对名称意义化的要求

证书主体DN项名称，所采用的用户标识信息，必须是真实、明确、可追溯、可查证的；对于OV SSL证书和EV SSL证书，其能单独或结合其他信息体现、反映、确定该个人、机构或设备的真实身份。

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。除非该假名注册在官方的有效登记证书中，可供SZCA查询、验证。

3.1.4 理解不同名称形式的规则

见本 CPS 的 7.1.4。

3.1.5 名称的唯一性

订户证书中的甄别名，唯一地标识具体订户身份。

3.1.6 商标的识别、鉴别和角色

未规定

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

订户拥有私钥，是通过pkcs#10格式的数字签名证书申请信息（certificate signing request,简称CRS）方法证明的。订户用私钥对证书申请信息签名并安全传输至SZCA，SZCA使用与订户私钥相对应的公钥进行签名验证，确认申请信息的完整性和签名的真实性，从而证明订户持有该私钥。

3.2.2 组织机构身份的鉴别

在申请组织机构的各类证书时，申请者应本人、或指定合法授权的证书申请代表，提交有效的身份证明文件，及与所申请证书类型相应的申请材料，并签署相关服务协议，同意承担相应的责任。

有效的个人身份证件包括：居民身份证、护照、驾驶证、军官等国家机关签发且含照片的有效身份证件；

机构身份证件，包括但不限于企业营业执照、组织机构代码证、法人登记证书、政府批文等机构成立合法有效的身份证明文件。

3.2.2.1 OV 证书

- 机构身份验证

根据机构提交身份证明文件，SZCA 将通过可靠第三方数据源；特许设立的，可向主管机关或上级组织查询，查询确认验证机构真实存在、合法有效。

- 证书申请意愿真实性及经办人授权验证

通过可信第三方获得机构的联系方式，联系机构确认证书申请的真实性，授权情况，及经办人/负责人的身份、联系方式。

3.2.2.2 EV 证书

EV 证书不接受包含通配符*的域名申请，不接受包含 IP 地址的申请。

EV 证书仅面向机构订户签发，不接受个人的证书申请，机构订户应满足以下条件：

1) 经机构注册管理机关合法注册设立，或经政府或上级组织许可、批准成立，且注册登记证明文件及经营资质文件，都处在有效期内；

2) 授权负责人、专门机构（如申请代理人、签署人、申请人、审批人，可一人兼任，可多人担任）负责申请证书；

3）未被登记机构等政府机构或司法机关等载入“停业”、“无效”、“过期”名单；

4) 有固定的经营场所和经营业务，并能够进行验证（对商业法人）；

5) 未被列入注册地政府任何黑名单或禁制名单中；

6) 经营所在地、注册地允许使用 SZCA 证书。

- 机构身份验证

除进行前述 OV 证书的验证外，还需对申请者在营业务的真实性进行验证。

为验证申请人实际有在开展经营，CA 应通过以下方式验证申请人、附属机构/母公司/子公司的在营业务：

（1）查证登记官方文件，如工商管理机构的年报等，验证申请人、附属机构、母公司或子公司已存续至少 3 年；或

（2）验证申请人、附属机构、母公司或子公司记入当前的政府信息源或税务信息源，存在纳税证明、记录等；

（3）通过受监管的金融机构直接出具的申请人、附属机构、母公司或子公司开设存款账户的证明文件，与受监管金融机构验证申请人、附属机构、母公司或子公司拥有在用的存款账户；或

（5）经营地所属物业公司开具的物业管理费用凭证、水电等公共服务机构开具的凭证。

SZCA接受申请后，检查证书申请材料，并审核订户身份的真实性，处理证书申请后

将依法留存与认证相关的订户材料、信息。

- 域名验证

（1）DV证书验证

对于DV证书而言，SZCA仅对证书申请者对该域名的所有权、使用权进行验证，不对申请者的身份作任何鉴别。

- 域名使用权、控制权验证

SZCA采用以下任一方法，验证申请者对域名的使用权、控制权：

1） 电子邮箱验证法

SZCA向所申请域名地址下的指定电邮地址(admin@域名,administrator@域名,webmaster@域名,postmaster@域名, hostmaster@域名)中的任一或多个地址，发送验证链接或验证码。

如申请者尚未创建改电邮地址的，应及时设置创建。或者SZCA通过WHOIS可公开查询记录获取到该域名的登记邮箱的，也可以该邮箱作为验证邮箱进行验证。

申请者点击SZCA发送至其电邮地址的验证链接，或返回该验证码，SZCA完成以电邮方式验证域名权限。

邮箱验证方式遵循 Baseline Requirments v 1.7.1 第 3.2.2.4.4 节要求。

2） 网页验证法

通过确认请求值或随机值出现于某个文件的内容中（例如，某个请求值或随机值不出现于用于收取该文件的请求中，并收从请求中收到成功的 HTTP 2xx 状态代码回复），以确认申请者对 FQDN 的实际控制权。

该鉴别方式遵循 Baseline Requirments v 1.7.1 第 3.2.2.4.18 节。

3） DNS TXT记录验证法

SZCA通过指定邮箱（已验证通过）向申请者发送随机值等验证码。

通过确认申请域名 在 DNS CNAME 、 TXT 或 CAA 记录中的任意值或请求令牌的存在来确认申请人对FQDN（完全限定域名）的控制。

该验证方式遵循 Baseline Requirmentsv 1.7.1 第 3.2.2.4. 7节要求。

4） 通配符域名验证

通过域名验证法，确认对通配符右侧域名的所有权、控制权，该域名归属于某商业实体、社会组织或政府机构，并经合法注册获得。

SZCA拒绝通配符右侧域名为顶级域名、公共域名或由域名注册管理机构控制的域名的证书申请，除非申请者能证明完全控制该域名。

上述随机验证码的有效期均为30天。

- IP 地址验证

对于 OV SSL 证书、DV SSL 证书，如 IP 地址载入证书内容，将采用在包含 IP 地址的 URI （统一资源标识符）的在线网页上，对约定的信息进行改动的方式，以确认申请者对 IP 地址的实际控制权 。

该鉴别方式遵循 Baseline Requirments v1.7.1 第 3.2.2.5.1 节。

3.2.3 个人身份的鉴别

- 个人身份验证：

对经办人提供的政府机构颁发的含照片的有效身份证件，如身份证、护照、军官证等，采用特定证件真伪鉴别技术手段，或经查询政府数据源或第三方可靠数据源，鉴别证件真伪有效性，检查申请人、经办人与证件照片一致性，及核对证件信息与申请信息的一致性。

- 与机构关系及经办人授权验证：

SZCA 通过从第三方可信数据源得到的电话号码、邮政信函等方式，与申请者进行联络，以确认被申请者某个信息的真实性，如验证代理人的职位或验证申请表中的某个人是否是申请人。

3.2.4 没有验证的订户信息

证书中的信息，未经 SZCA 验证不写入证书。

3.2.5 授权确认

当法人等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。SZCA有权通过第三方或其它方式确认被授权人的信息，亦有权要求被授权人提供授权委托书等额外的信息证明材料，验证申请人代表申请证书的真实性，包括对申请人代表的授权文件，及申请证书的意愿确认。

3.2.6 互操作准则

未规定

3.3 密钥更新请求的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

在证书内容不变的情况下，如在证书有效期即将届满或到期，订户需要在证书期满后继续使用证书的；或对证书密钥有安全顾虑时，可以申请重新注册、产生新的密钥对，并向 SZCA 申请重新签发证书。

对于常规密钥的更新，在订户提交经原证书签名的证书请求文件 CSR，及原证书甄别名、序列号等基本证书信息后，SZCA 查询、核实原证书是否真实存在且由 SZCA 签发，使用原证书公钥验证申请签名，并基于原申请信息验证订户身份。

证书密钥需要更新的情形，主要是证书有效期即将届满或已到期，且证书密钥安全。证书更新，为保证安全性密钥也同时更新。

3.3.2 吊销后密钥更新的标识与鉴别

证书被吊销后申请密钥更新相当于订户申请新证书，即证书吊销后对密钥更新的标识与鉴别按照本 CPS 3.2 处理。

3.4 吊销请求的标识与鉴别

对于订户及其代理人提出的证书吊销请求，具体识别与鉴别程序按照本 CPS 4.9.3 进行。

对吊销申请的标识与鉴别，只适用于订户提出吊销申请。对于 SZCA 依据充足的事实和理由，以及根据司法机关的证书吊销裁决等作出的证书吊销，无需进行身份鉴别。

4. 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

个人、法人或非法人组织，均可申请 SZCA 证书。

4.1.2 注册过程与责任

最终订户即申请证书的实体。

最终订户需要按照本 CPS 3.2.2 的要求提供真实、准确、完整的申请材料、信息，包括申请表（如有）、身份证明材料；最终订户须明确表示其愿意接受本 CPS 、及相关 CP （如有）（SZCA 在官网公布 CPS，及其 CP）中所规定的相关责任与义务，同意遵循并签署订户服务协议。

若申请人提交的申请信息不足，SZCA 有权从申请人处，或从可靠第三方处获得证书必要的其他信息，并经申请人确认。

SZCA 及其注册机构（如有）对订户提供的身份信息按照本 CPS3.2.2 的要求进行鉴别，SZCA 及 RA 机构对通过鉴别后的订户签发证书。SZCA 将妥善保管证书订户申请材料、信息。SZCA 的注册机构应在适当时间将证书订户的信息归档，同时履行本 CPS 中所规定的相关责任与义务。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

SZCA 处理证书申请至少需要设置三个可信角色：信息收集录入、信息审核验证、签发证书。且信息审核验证角色与证书签发实行职责分离，不能由同一主体完成。

对于根据第 3.2 节获得的数据、文档，或之前签发证书产生的验证信息，SZCA 可重复使用进行新证书颁发，前提是从第 3.2 节规定的来源获得信息，或验证信息和材料时效未超过 398 天并且未有变化。

4.2.2 证书申请批准和拒绝

对于申请 SSL 证书的用户，SZCA 在用户身份认证、域名/IP 地址控制验证之外，还将采取合理措施检查该域名是否为完全合格域名，及其查看域名系统的 CAA 记录配置。

对于 SZCA 颁发的 满足 CA/ 浏览器论坛 EV Guidelines 、 Baseline Requirements 要求的公共可信任的 SSL/TLS 证书， SZCA 对签发证书主题别名扩展项中的每一个 dNSName 做 CAA 记录检查 ，并遵循查询到的指示 。

SZCA 根据 RFC6844 （经勘误表 5065 修订） 的规定处理“ issue ”、“issuewild ”及“iodef ”的属性标签， 若“ issue ”、 “issuewild ”标签中不包含 “szca.com”，则 SZCA 不签发对应的证书 ；若 CAA 记录中出现“ iodef ”标签，则 SZCA 与申请者沟通后决定是否为其颁发证书 。

SZCA 以下列 CAA 记录查找失败情况作为可签发证书的条件： 1 ）在非 SZCA 的基础设施中查询 CAA 记录失败； 2 ）至少尝试过一次重新查找 CAA 记录； 3 ）域名所在区域不存在指向 ICNNA 根区域的 DNSSEC 验证链。

接受到申请后，SZCA 将检查其是否处于高风险域名清单，是否属于因涉嫌网络钓鱼或其他欺诈犯罪活动或疑虑而曾被吊销证书或拒绝证书请求，并标记该证书申请的情况。

对于申请 ICANN 正在审议，且仅仅用于内部自用的新 gTLD（通用顶级域名）证书，SZCA 拒绝该证书申请。

SZCA 按照本 CPS 3.2 的要求对订户提交的申请材料及其身份信息进行鉴别，经鉴别符合要求后，将批准申请，并为订户签发证书。若申请材料不足，或鉴别未通过，SZCA 将拒绝其申请，及时通知申请者并告知理由。

4.2.3 处理证书申请的时间

在申请者所提交的证书申请材料齐全完整并符合要求的情况下，SZCA 或授权的注册机构将在 3 个工作日内处理证书申请，如有特殊情况，可适当延长证书处理时间，但最长不得超过 7 个工作日。EV 证书的申请处理时间最长不超过 15 日。

4.3 证书签发

4.3.1 证书签发中注册机构和电子认证服务机构的行为

在订户申请通过鉴别后，RA 系统操作员录入订户申请信息，并提交 RA 系统审核员审核； RA 审核通过后，向 CA 系统提交申请；CA 系统向 RA 系统返回证书下载凭证码或证书，由 CA 或注册机构以安全的形式将证书或证书下载凭证码反馈给订户。

4.3.2 电子认证服务机构和注册机构对订户的通告

无论是批准还是拒绝订户的证书申请，SZCA 有义务告知订户申请的处理结果。SZCA 将以电话、电子邮件或其他安全可行方式对订户进行通告。

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 或授权的注册机构将向申请者提供证书、或证书的获取渠道。由 SZCA 获订户授权代为持有、安装使用证书的，SZCA 将及时将证书以电邮、短信、站内信等方式将证书交订户检查确认。

证书申请者通过上述方式获得证书后，应检查、测试使用证书是否存在内容错误、安装使用异常等问题；若发现证书问题，应在 2 个工作日内通知 SZCA 提出异议。订户在获得证书起的未提出异议或提出的异议被认定不成立，无论是否下载、安装、使用证书，即被视为

已接受证书。

4.4.2 电子认证服务机构对证书的发布

SZCA 签发完成的证书，将按照订户意愿进行证书的发布。

4.4.3 电子认证服务机构对其他实体的通告

对于 SZCA 签发的证书，SZCA 及其授权注册机构不对其他实体进行通告。依赖方有需要的可以自行在信息库上查询。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户的私钥和证书应用于法律、CPS 规定的、或服务协议约定的用途（见本 CPS1.4.1 ），不得将证书用于实施违法犯罪活动；

订户在使用证书时必须遵守本 CPS 的要求，妥善保存其私钥，保持本人对私钥的控制，采取合理的措施防止私钥遗失、泄露、被篡改，避免他人未经本人授权而使用本人证书情形的发生，否则其应用是不受保障的。订户在发生无法确定证书及其私钥是否安全的事件或意外时，应立即通知 SZCA 吊销该证书。

订户使用证书私钥签名，即保证是以订户本人名义进行的签名，且在进行签名时证书未过期、未被吊销。证书持有者在证书到期不续费或被吊销后，须停止使用该证书对应的私钥。

4.5.2 信赖方公钥和证书的使用

依赖方信赖 SZCA 签发的 SSL 证书所证明的信任关系时，需要：

（1）获得数字签名对应的 CA 机构证书和信任链；

（2）查询 CRL 或 OCSP，确认数字签名对应的证书有效、状态正常；

（3）确认 CA 机构证书是依赖方信任的证书；

（4）证书的用途适用于对应的签名；

（5）使用证书上的公钥验证签名。

以上任一条件不满足或步骤操作失败，依赖方应该拒绝接受签名信息。

4.6 证书更新

4.6.1 证书更新的情形

当订户证书即将到期，且密钥安全时，可为订户签发新证书；

4.6.2 请求证书更新的实体

见本 CPS 4.1.1。

4.6.3 证书更新请求的处理

订户在证书有效期届满前 30 天申请证书更新的，应立即向 SZCA 申请证书密钥更新。

证书更新处理程序如下：1）验证原证书真实性，是否由 SZCA 签发；

2）检查证书更新请求是否在约定的续期期间提出；

3）若原证书申请材料、身份证明文件自提供至请求证书更新未超过 398 天，且信息内容未发生变化时，SZCA 可重用该材料、身份证明文件，免于订户提供申请材料和证明文件进行身份鉴别。

4）订户可用原证书私钥对 CSR 证书更新请求文件进行签名，并配合原证书的序列号、甄别名等原证书关键信息，SZCA 将对密钥对、及更新请求内的用户信息进行确认验证。

4.6.4 颁发新证书时对订户的通告

同本 CPS 4.3.2。

4.6.5 构成接受更新证书的行为

同本 CPS 4.4.1。

4.6.6 电子认证服务机构对更新证书的发布

同本 CPS 4.4.2。

4.6.7 电子认证服务机构对其他实体的通告

同本 CPS 4.4.3。

4.7 证书密钥更新

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：

1) 密钥对已经、或怀疑泄漏、被窃取、被篡改或出现其它密钥对安全性无法得到保障的情形；

2) 证书被吊销后新申请证书。

4.7.2 请求证书公钥更新的实体

见本 CPS4.1.1。

4.7.3 证书密钥更新请求处理

见本 CPS3.3。

SZCA 为用户生成新证书并传送给用户。

4.7.4 颁发新证书时对订户的通告

见本 CPS4.3.2。

4.7.5 构成接受密钥更新的行为

见本 CPS4.4.1

4.7.6 电子认证服务机构对密钥更新证书的发布

见本 CPS4.4.2。

4.7.7 电子认证服务机构对其他实体的通告

见本 CPS4.4.3。

4.8 证书变更

证书变更是指在证书未到期之前，证书除公钥及有效期之外的其他订户信息发生变化而重新办理证书。SZCA 的认证业务不直接支持证书变更。订户证书内容变化且订户申请变更证书的，视为新申请证书。需要先将原有证书吊销，且证书的申请及处理流程与申请新证书一致。

4.8.1 证书变更的情形

当企业、政府机构、事业单位及其他非法人组织订户的信息发生变化，造成实体身份发生变化时，用户须及时通知 SZCA 申请办理证书变更，吊销原证书并签发新证书。

4.8.2 请求证书变更的实体

已申请证书的主体，可申请证书变更。

4.8.3 证书变更请求的处理

同本 CPS 4.2。

4.8.4 颁发新证书时对订户的通告

同本 CPS 4.3.2。

4.8.5 构成接受变更证书的行为

同本 CPS 4.4.1。

4.8.6 电子认证服务机构对变更证书的发布

同本 CPS 4.4.2。

4.8.7 电子认证服务机构对其他实体的通告

同本 CPS 4.4.3。

4.9 证书吊销

4.9.1 证书吊销的情形

如有下列任何一种情况发生，则订户的证书将被吊销：

（1）订户书面申请吊销数字证书；

（2）订户未支付证书费用；

（3）订户通知 CA 且有证据证明初始的证书申请未获有效授权；

（4）订户相信或怀疑密钥泄漏或遭受攻击，存放证书的服务器损坏或被锁定等情形；或者 CA 有证据表明订户证书私钥泄露的情形；

（5）当 CA 有证据表明订户将证书使用于法律法规禁止的违法犯罪事项上，或者 CA 发现订户证书未恰当使用；

（6）当 CA 有证据表明订户未履行本 CPS 或订户协议中约定的义务；

（7） CA 发现且有合理证据证明订户证书中的重要信息内容已经变更；

（8）CA 签发的证书未能满足证书策略或证书标准中的要求和条件；

（9）CA 认定证书中所显示的信息为不真实、不准确或具有误导性，证书密钥不匹配的；或者订户申请证书时，提供的资料不真实；

（10）CA 因某些原因停止业务，并且没有安排其他的 CA 提供证书吊销服务；

（11）CA 用于签发证书的 CA 证书私钥可能被泄露时，将根据应急预案吊销所有已签发的证书；

（12）CA 有合理证据表明或意识到订户已经被列在相关的黑名单中，或其经营地区被 SZCA 所在国家的监管机构禁止；

（13）证书的重要参数被国际国内主流标准认为有重大风险时；

（14）CA 发现证书被用于欺诈性误导性域名；

（15）CA 发现并查实订户丧失对域名、IP 地址的所有权或使用权，如依法院裁判或仲裁机构仲裁吊销域名注册人权利，申请人与域名注册人的使用授权协议终止，或有证据证明之前的域名或 IP 地址验证结果不可信；

（16）法律、行政法规规定的其他情形。

4.9.2 请求证书吊销的实体

已申请 SZCA 证书的订户可请求证书吊销。依赖方、软件商或其他第三方提供合理证据，可申请吊销证书。CA 机构及其注册机构可主动吊销证书。

4.9.3 请求吊销的流程

订户提出吊销申请，并提供吊销原因说明，由 SZCA 按本 CPS3.4 审核通过后吊销证书。如依赖方、浏览器厂商等发现证书密钥不安全或使用不合法的，可向 SZCA 反映问题。

SZCA 证书吊销联系人：张晓霞，电话：0755-26588399 转 892，联系邮箱：report@szca.com 。

SZCA 在发现本 CPS 4.9.1 第（1）、（3）、（4）项外的情形的，因订户的违法使用证书、密钥失密或证书信息发生重大变化等原因，且调查属实，可直接决定吊销证书。

SZCA 或其授权注册机关等根据司法机关的裁决，进行调查核实后吊销证书。但对于此种非经订户申请吊销的强制吊销，SZCA 或其发证机构将对相关的裁判文书及其他有效法律文件进行严格核验，并在机构内部经过至少两级的逐层审批，并由高级管理人员完成最终审批。

证书吊销后，SZCA 将通过电话、电邮、短信等方式通知订户证书吊销的事实及告知理由。

4.9.4 吊销请求宽限期

订户一旦发现需要吊销证书，应及时向 SZCA 提出吊销请求，但最迟不得于自发现证书应吊销起的 8 个小时。否则延迟申请期间证书相关损失由订户承担。

SZCA 吊销证书的，订户在收到吊销通知后的 3 个工作日内可向 SZCA 提出异议，但需同时说明理由或提供证据；SZCA 将会对异议进行审查，若确认其理由正当则不予以吊销；若订户规定时间内未提出异议或异议不成立的，则 SZCA 将予以吊销。

4.9.5 电子认证服务机构处理吊销请求的时限

证书订户申请吊销证书的，SZCA 收到吊销请求并审核完成后，24 小时内吊销证书。

强制吊销情况下，订户在收到吊销通知后的 3 个工作日内可向 SZCA 提出异议；若订户在 3 个工作日内未回复、无异议或异议不成立，则 SZCA 将于 3 个工作日满后的 24 小时内予以吊销。

经用户、应用软件提供商，或其他第三方报告证书相关问题，或通知吊销证书的，SZCA 应在收到问题报告、通知后的 24 小时内，将相关的事实情况、调查结果形成报告，向订户、报告通知实体提供；并与其商议证书吊销时间，但不得晚于 24 小时。

4.9.6 依赖方检查证书吊销的要求

SZCA 提供在线证书状态吊销查询服务，依赖方可通过 SZCA 网站查询。

4.9.7 CRL 发布频率

SZCA 证书吊销列表在 24 小时内自动更新，特殊紧急情况下可以通过手动方式变更 CRL 列表。且下一次更新时间字段与本次更新时间相隔不得超过 10 天。中级 CA 的 CRL，即根签发的 CRL 列表，发布周期是 12 个月，下次更新和本次更新时间相隔不超过 12 个月。

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 在线状态查询的可用性

SZCA 提供证书状态的在线查询服务，该服务维持 7X24 小时不间断可用。

4.9.10 在线状态查询要求

信赖方是否进行在线状态查询完全取决于信赖方的安全要求。对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，信赖方在信赖一个证书前可通过证书状态在线查询系统检查该证书的状态。

订户证书， SZCA 的 OCSP 响应最短有效期不低于 1 天，最长有效期不超过 10 天，SZCA 在 OCSP 本次更新时间后的 4 天以内，距下次更新时间的至少 8 小时之前进行信息更新。

中级 CA 证书，SZCA 至少每 12 个月更新 OCSP 信息。当吊销中级 CA 证书时，在 24 小时内更新 OCSP 信息。

对于未签发的证书的状态查询请求，SZCA 不返回“good”状态。

4.9.11 吊销信息的其他发布形式

除 CRL、OCSP 服务外，SZCA 不提供其他发布形式的吊销信息。

4.9.12 密钥损害的特别要求

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向 SZCA 申请证书吊销。

4.9.13 证书挂起的情形

未规定

4.9.14 请求证书挂起的实体

未规定

4.9.15 请求挂起的流程

未规定

4.9.16 证书挂起的时限

未规定

4.10 证书状态服务

4.10.1 操作特征

证书的状态信息，SZCA 通过 OCSP、CRL 服务提供。订户或依赖方，可以通过登录 SZCA 网站在线访问 OCSP 服务器，或从 SZCA 网站或 LDAP 下载 CRL 到本地，对证书的状态进行查询。

4.10.2 服务可用性

SZCA 提供 7X24 小时的证书状态查询服务。证书状态查询请求响应时间不超过 10 秒。

4.10.3 可选特征

未规定

4.11 订购结束

订购结束的情形有以下两种：

（1）证书到期时且不续费申请使用其他证书服务；

当证书到期时，订户不续费不申请更新证书，不再使用 SZCA 证书。

（2）证书有效期内吊销证书。

在证书有效期内，出现下列任一证书吊销情形的，证书使用者与 SZCA 的服务终止：

① 证书使用者由于自身原因而单方面申请吊销证书，SZCA 审核通过后决定吊销证书；

② 或者司法机关裁决吊销证书，并向 SZCA 提出执行请求；

③ SZCA 根据 CPS 或用户协议吊销该证书。

4.12 密钥托管与恢复

4.12.1 密钥托管和恢复的策略及行为

订户签名密钥对由订户的密码设备生成，由订户自行保管。订户应妥善保管签名密钥，对其进行备份，由于签名私钥遗失所造成的损失由订户自己承担。SZCA 不归档、备份订户的签名私钥，签名密钥无法恢复。

4.12.2 会话密钥的封装和恢复的策略与行为

未规定

5.认证机构设施、管理和操作控制

5.1 物理控制

SZCA 的认证服务系统处于安全稳固的建筑物内，具备独立的软硬件操作环境。且系统及设备等物理环境，配备有预防水患、火灾、电磁干扰与辐射及其他自然灾害、工业事故的各种装备、设施。

SZCA 实施功能分区及其访问控制制度，操作人员要进入、操作相应的管理区域及其他关键核心区域，必须进行身份认证，且被视频监控监测记录；且对该区域的设备与系统日常运行及人员操作过程进行监控。SZCA 的根密钥置于最高安全强度保护环境与状态，防止任何非法破坏或者未经授权的操作。SZCA 的核心 CA 系统及中级 CA 系统所使用的相关设备均有四道以上门禁系统做保护。

5.1.1 场地位置与建筑

SZCA 的建筑物和机房建设按照下列标准实施：

GB/T 25056-2010《信息安全技术证书认证系统密码及其相关安全技术规范》

GM [2010]《电子政务电子认证基础设施建设要求》

GB50174-2008《电子信息系统机房设计规范》

GB6650-1986：《计算机机房用活动地板技术条件》

GB2887-2011《计算机场地通用规范》

GB30003-93《电子计算机机房施工及验收规范》

GB50222-95《建筑内部装修设计防火规范》

GB50116-98《火灾自动报警系统设计规范》

GB50057-94《建筑物防雷设计规范》

GB5054-95《低压配电设计规范》

GB/J19-87《采暖通风与空气调节设计规范》

SJ/T10796-1996《计算机机房用活动地板技术条件》

YD/T754-95《通讯机房静电防护通则》

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，机房按照功能划分为多个功能区。各功能区域对应的安全区域，实施不同的安全等级控制制度，SZCA 采用门禁控制、视频监控等多种有效的物理安全控制措施。机房具备抗震、防火、防水、恒湿温控、防电磁干扰与辐射、备用电力等功能，保障服务的连续性、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。

操作人员进出每一道门都有时间记录和相关信息提示，服务区与核心区需要两个管理员同时使用身份识别卡和指纹鉴别才可以进入，机房工作人员按照机房日常工作规范，每月对门禁记录进行整理归档，保留一年的门禁记录。

物理访问控制包括如下几个方面：

（1）门禁系统：控制各层门的进出。操作人员需使用身份识别卡或结合口令或指纹鉴定才能进出，进出每一道门应有时间纪录和信息提示。

（2）报警系统：当发生任何非法闯入、非正常手段的开门、长时间不关门等异常情况都应触发报警系统。

（3）监控系统：与门禁和物理侵入报警系统配合使用的还有录像监控系统，对安全区域和操作区域进行 7*24 小时不间断录像。所有录像资料至少保留 6 个月，以备查询。

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和解决新风供应以及机房对空气清洁度的要求等问题。

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，一旦发生水患立即报警，通知有关人员采取应急措施，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 废物处理

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。

5.1.8 异地备份

SZCA 对重要数据、审计日志数据和其他敏感信息进行异地备份，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

在 SZCA 提供电子认证服务过程中，能从本质上影响证书的颁发、使用、管理和吊销等涉及密钥操作的职位都被 SZCA 视为可信角色。这些角色包括但不限于：密钥和密码设备的管理人员、系统管理人员、安全审计人员、业务管理人员及业务操作人员等，具体岗位名称和要求以 SZCA 的岗位设置及其说明为准。

5.2.2 每项任务需要的人数

SZCA 在具体业务规范中对关键任务进行严格控制，敏感操作需要多个可信角色共同完成，例如：

（1）密钥和密码设备的操作和存放：需要 3 个可信人员中的至少 2 个共同完成；

（2）证书签发系统的后台操作：需要 3 个系统管理人员中的至少 2 个可信人员共同完成；

（3）审核和签发证书：需要 2 个可信人员共同完成。

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	3
10	录入员	若干
11	审核员	1
12	制证员	1

5.2.3 每个角色的识别与鉴定

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。

5.2.4 需要职责分割的角色

为保证系统安全，遵循可信角色分离的原则，即 SZCA 的可信角色由不同的人担任。SZCA 进行职责分离的角色，包括但不限于下列角色：

（1） 证书业务受理

（2） 证书或 CRL 签发

（3） 系统工程与维护

（4） CA 密钥管理

（5） 安全审计。

5.3 人员控制

5.3.1 资质、经历和无过失要求

SZCA 对承担可信角色的工作人员的资格要求如下：

（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和良好的从业经历。

（5） 具备良好的团队合作精神。

（6） 无违法犯罪记录。

（7） 关键和核心岗位的工作人员必须具备相关的工作经验，或通过 SZCA 相关的培训和考核后方能上岗。

5.3.2 背景调查程序

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 根据可信角色的职位需求，给予相应的岗前培训，综合培训内容如下：

（1） SZCA 运营体系；

（2） SZCA 技术体系；

（3） SZCA 安全管理策略和机制；

（4） 岗位职责统一要求；

（5） PKI 基础知识；

（6） 身份验证和审核策略和程序；

（7） 灾难恢复和业务连续性管理；

（8） CP、CPS 政策及相关标准和程序；

（9） SZCA 管理政策、制度及办法等；

（10） 国家关于电子认证服务的法律、法规及标准、程序；

（11） 其他需要进行的培训等。

SZCA 将员工参加培训的情况形成记录并存档，对于签发 SSL 服务器证书和代码签名证

书的操作员和审核员，上岗前必须通过培训并达到 Baseline Requirement 中要求的从事该项工作所必须的技能水平。

5.3.4 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受 SZCA 组织的培训一次。对于认证系统运营相关的人员，每年至少进行一次相关技能和知识培训。此外，SZCA 将根据机构系统升级、策略调整等要求，不定期的要求人员进行继续培训。

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。并视该人员未授权行为的情节严重性，实施对该名人员的通报批评、罚款、辞退以及提交司法机构处理等措施。

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

所有发生在 SZCA 的重大安全事件都会自动地打上时间印章并记录在审计跟踪档案中，这些记录，不论是手动生成或者是系统自动生成，都应该包含以下信息：

（1）事件发生的日期和时间；

（2）记录的序列号；

（3）记录的类型；

（4）记录的来源；

（5）记录事件的实体。

这些事件包括但不限于：

（1） 密钥生命周期内的管理事件，包括密钥生成、备份、存储、恢复、使用、吊销、归档、销毁、私钥泄露等；

（2） 密码设备生命周期内的管理事件，包括设备接收、安装、卸载、激活、使用、维修等；

（3） 证书申请事件，包括订户接受订户协议，接受申请的单位、申请资料的验证、申请及验证资料的保存等；

（4） 证书生命周期内的管理事件，包括证书的申请、批准、更新、吊销等；系统安全事件，包括：成功或不成功访问 CA 系统的活动，对于 CA 系统网络的非授权

访问及访问企图，对于系统文件的非授权的访问及访问企图，安全、敏感的文件或记录的读、写或删除，系统崩溃，硬件故障和其他异常；

（5） 防火墙和路由器记录的安全事件；

（6） 系统操作事件，包括系统启动和关闭，系统权限的创建、删除，设置或修改密码；

（7） CA 设施的访问，包括授权人员进出 CA 设施、非授权人员进出 CA 设施及陪同人和安全存储设施的访问；

（8） 可信人员管理记录，包括网络权限的帐号申请记录，系统权限的申请、变更、创建申请记录，人员情况变化。

5.4.2 处理日志的周期

SZCA 每周进行一次日志跟踪处理，检查违反政策及其它重大事件，每月进行发证系统日志分析。所有的审计日志定期由专人进行检查和审阅，以便发现重要的安全和操作事件，及时采取相应的措施进行处理。

5.4.3 审计日志的保存期限

SZCA 妥善保存电子认证服务的审计日志，保存期限为证书失效后七年。

5.4.4 审计日志的保护

SZCA 执行严格的物理和逻辑访问控制措施，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 的审计跟踪文档由业务管理员和审计人员每月进行审计日志和审计文档的归档备

份。所有文档包括最新的审计跟踪文档应储存在磁盘中并存放在安全的文档库内。

5.4.6 审计收集系统

SZCA 设置自动审核系统以审核记录与资料，自动向有关人员或系统报告审核事件。

（1） 审计日志收集系统；

（2） 证书管理系统；

（3） 证书签发系统；

（4） 证书目录系统；

（5） 远程通信系统；

（6） 访问控制系统；

（7） 网站、数据库安全管理系统；

（8） 其他需要审计的系统。

5.4.7 对导致事件实体的通告

SZCA 发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

SZCA 有权决定是否对导致事件的实体进行通告。

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，对于薄弱环节，SZCA 每季度对系统进行例行性质的技术漏洞评估，并针对评估结果进行相应处置，以降低

系统运行的风险。认证系统本身以及支持认证系统安全运维的相关技术资源，若发生重大变更，亦针对变更项目进行例外性质的技术漏洞评估，确保变更未衍生相应重大技术漏洞。

5.5 记录归档

5.5.1 归档记录的类型

SZCA 对以下几类事件进行归档记录，包括但不限于：

（1） 证书系统建设和升级文档；

（2） 证书和证书吊销列表；

（3） 证书申请支持文档，证书服务批准和拒绝的信息，与证书订户的协议；

（4） 审计记录；

（5） 证书策略、电子认证业务规则文档；

（6） 员工资料，包括但不限于背景调查、录用、培训等资料；

（7） 各类外部、内部评估文档。

5.5.2 归档记录的保存期限

SZCA 对于不同的归档记录，其保留期限是不同的。

（1）对订户证书生命周期内的管理事件的归档，保留 7 年以上。

（2）对 CA 证书和密钥生命周期内的管理事件的归档，其保留期限不少于 CA 证书和密钥生命周期。

（3）订户证书的归档保留期限不少于证书失效后 7 年。

（4）CA 证书和密钥的归档在 CA 证书和密钥生命周期之外，额外保留 7 年。

（5）对于系统操作事件和系统安全事件记录，其归档应保留 7 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

对于系统生成的电子归档记录，每周进行备份，备份文件进行异地存放。

对于书面的归档资料，不需要进行备份，但需要采取严格的措施保证其安全性。

所有归档的电子文件和数据库除了保存在 SZCA 的存储库，还在异地保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有被授权的工作人员或在其监督的情况下，才能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 记录时间戳的要求

SZCA 的档案在创建的时候须加盖时间戳。

5.5.6 归档收集系统

SZCA 的审计跟踪档案收集系统在本 CPS 第 5.4 节中作详细说明。

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

在证书到期以前，SZCA 将按照证书策略的规定对根密钥进行更换，生成新的证书。在

进行密钥的生成时，严格按照 SZCA 关于密钥管理的规范。CA 密钥更替必须遵循以下原则：

（1） 在 CA 证书生命周期结束前停止签发新的下级证书，确保在 CA 的证书到期时所有下级证书也全部到期。

（2） 在停止签发新的下级证书后至证书到期时，继续使用 CA 私钥签发 CRL，直到最后一张下级证书过期。

（3） 生成和管理 CA 密钥对时，严格遵守密钥规范。

（4） 及时发布新的 CA 证书。

确保整个过渡过程安全、顺利，不出现信任真空期。

5.7 损害与灾难恢复

当 SZCA 遭到攻击，发生通信网络资源崩溃、毁坏、故障，及计算机设备系统不能正常提供服务，软件被破坏、数据库被篡改等情形或因不可抗力造成 SZCA 机房服务暂停或瘫痪时，SZCA 将依照《SZCA 灾难恢复计划》规定的事故处理、紧急应变、灾难恢复和业务持续运作的程序和应对措施实施恢复。并根据要求向 CA 机构的审计人员提供业务连续性和安全计划，并每年测试、审查和更新该程序。

5.7.1 事故或损害处理程序

为了及时响应和处理事故和损害发生的情况，SZCA 建立了一系列应急处理预案和事故处理方案，例如：《SZCA 系统故障处理规范》、《SZCA 重大事故应急预案》、《SZCA 系统备份与恢复方案》。

相关岗位的工作人员将按照以上方案和相关制度的规定，积极实施抢修恢复计划和措施，每季度进行数据灾难恢复演练，每年进行一次重大事故应急演练。

5.7.2 计算机资源、软件或数据的损坏

SZCA 对业务系统及其他重要系统的资源、软件及数据进行了备份，并制定了相应的应急处理流程。当发生网络通信资源毁坏、计算机设备不能提供正常服务、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 将按照灾难恢复计划实施恢复。

5.7.3 实体私钥损害处理程序

在故意的、人为的或是自然灾难的情况下，SZCA 将采取下列步骤以恢复安全环境：

（1）SZCA 认证系统的口令由业务管理员、业务操作员、系统管理员进行变更；

（2）根据灾难的性质，部分或全部证书需要吊销或之后重新认证；

（3）如果目录无法使用或者目录有不纯的嫌疑，目录数据和 CRL 需要进行恢复；

（4）及时访问安全现场尽可能合理地恢复操作；

（5）如果需要恢复业务管理员的配置文件，应由系统管理员执行恢复。

如果需要恢复 SZCA 业务操作员的配置文件，则由另外一名 SZCA 安全业务操作员或业务管理员对其进行恢复。

当 CA 根私钥被攻破、遗失、被篡改或泄露，SZCA 启动重大事件应急处理程序，制定行动计划。如果需要吊销 CA 证书，将会采取以下措施：

（1）立即向电子认证服务管理办公室和其他政府主管部门汇报，通过网站和其他公共媒体对订户进行通告，采取措施避免用户利益遭受更大损失；

（2）立即通知相关依赖方关闭与证书认证服务相关的系统；

（3）立即吊销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。同时 SZCA 立即生成新的密钥对；

（4）新的根证书签发后，按照 SZCA CPS 关于证书签发的规定，重新签发下级证书和下级操作中级 CA 证书；SZCA 新的证书签发后，将立即通过 SZCA 信息库、目录服务器、HTTP

等方式发布。

当中级 CA 私钥出现遗失、被篡改、破解、泄露或被第三者窃用的疑虑时，操作 CA 立即向 SZCA 进行汇报并生成新的密钥对和证书请求，申请签发新的证书；

（1）SZCA 立即向电子认证服务管理办公室和其他政府主管部门汇报，通过网站和其他公共媒体对订户进行通告，采取措施避免用户利益遭受更大损失；

（2）立即通知相关依赖方关闭与证书认证服务相关的系统；

（3）立即吊销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询；

（4）新的中级 CA 证书签发后，按照 SZCA CPS 关于证书签发的规定，重新签发订户证书；

（5）SZCA 新的证书签发后，将立即通过 SZCA 信息库、目录服务器、HTTP 等方式进行发布。

证书订户的私钥可能出现损毁、遗失、破解、被篡改，或者被第三者窃用时，订户应按照 SZCA CPS 的规定，首先申请证书吊销，并按照规定重新申请新的证书。

5.7.4 灾害后的业务连续性能力

SZCA 在遭遇本节 5.7.1、5.7.2 和 5.7.3 中描述的灾难后，通过其备份机制，将在 24 小时之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

SZCA 终止事件的原因可以分为密钥受损原因和非密钥受损原因，密钥受损原因可能包括 SZCA 根密钥丢失，非密钥受损原因可能与商业因素有关。

在 SZCA 终止前，必须：

（1） 委托业务承接单位；

（2） 起草 SZCA 终止声明；

（3） 通知与 SZCA 停止相关的实体；

（4） 关闭从目录服务器；

（5） 证书吊销；

（6） 处理存档文件记录；

（7） 停止认证中心的服务；

（8） 存档主目录服务器；

（9） 关闭主目录服务器；

（10） 处理 SZCA 业务管理员和 SZCA 业务操作员；

（11） 处理加密密钥；

（12） 处理和存储敏感文档；

（13） 清除 SZCA 主机硬件。

由于密钥受损和非密钥受损原因而终止 SZCA，几乎要完成相同的操作，唯一的不同在 SZCA 终止发送通知的时间限制上，由于密钥受损原因终止 SZCA，要求 SZCA 通知订户的过程尽快完成；由于非密钥受损原因终止 SZCA，在 SZCA 通知所有订户后，采取适当的步骤减轻 SZCA 终止对订户的影响。

6.认证系统技术安全控制

6.1 密钥对的生成与安装

6.1.1 密钥对的生成

CA 密钥对由国家密码主管部门批准和许可的设备生成的。密钥的生成、管理、存储、备份和恢复应遵循FIPS140-2标准的相关规定。由于FIPS140-2标准并非是国家密码主管部门认可和支持的标准，国家对于密码产品有严格的管理要求，因此FIPS140-2标准仅参照执行，是在国家密码管理政策许可前提下的选择性适用，具体参照设备厂商提供的资料。用于此类密钥生成的密码模块须通过国家密码主管部门鉴定、认证。

订户密钥对由订户自身的服务器或其它设备内置的密钥生成机制生成。SZCA可接受为订户生成密钥对和CSR，私钥加密保护后通过SSL加密连接传送给订户。订户密钥生成将由可信角色在使用了合适的随机数生成器或伪随机数生成器并满足或超过FIPS 140-2第二级别要求的加密设备中操作。密钥长度至少为RSA 2048位或ECC 256位。在SZCA网站使用私钥生成工具所产生的风险由订户承担。SZCA不保存任何私钥和密码，所有这些信息在传送给用户后删除。

证书订户负有保护私钥安全的责任和义务，并承担由此带来的法律责任。

6.1.2 私钥传送给订户

私钥由订户自行生成，SZCA 不需要将私钥传递给订户。SZCA 可接受为订户生成密钥对和 CSR，私钥加密保护后通过 SSL 加密连接传送给订户。

6.1.3 公钥传送给证书签发机构

订户通过 PKCS#10 格式的证书签名请求信息或其它数字签名的文件包格式，以电子的方式将公钥提交给 SZCA 签发。

6.1.4 电子认证服务机构公钥传送给依赖方

SZCA 的公钥包含在 SZCA 自签发的根 CA 证书和业务 CA 证书中，通过 SZCA 官方网站进行发布。SZCA 支持从 SZCA 的网站下载的方式传递公钥，以供证书订户和依赖方查询使用。

6.1.5 密钥的长度

SZCA 支持的 RSA 密钥长度为 2048 位或以上，支持的 SM2 密钥长度为 256 位，支持的 ECC 密钥长度为 256 或以上。如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，SZCA 将会完全遵从。

6.1.6 公钥参数的生成与质量检查

对于使用硬件密码模块的 SZCA 订户，公钥参数必须使用国家密码管理局批准许可的加密设备和硬件介质生成，例如加密机、加密卡、USB Key、IC 卡等生成和选取，并遵从这些设备的生成规范和标准。SZCA 认为这些设备和介质内置的协议、算法等已经具备了足够的安全等级要求。

对于参数质量的检查，同样由通过国家密码管理局批准许可的加密设备和硬件介质进行，例如加密机、加密卡、USB Key、IC 卡等。SZCA 认为这些设备和介质内置的协议、算法等已经具备了足够的安全等级要求。

6.1.7 密钥使用目的

SZCA 的根 CA 密钥仅用于签署以下证书：

（1）代表根 CA 的自签证书；

（2）中级 CA 的证书及交叉证书；

（3）用于基础设施的证书（如 OCSP 响应验证证书）。

订户的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 私钥保护与密码模块工程控制

6.2.1 密码模块标准与控制

SZCA 所用的密码设备都是经国家密码管理局认可的产品。密钥的生成、管理、存储、备份和恢复应遵循 FIPS140-2 标准的相关规定。由于 FIPS140-2 标准并非是国家密码主管部门认可和支持的标准，国家对于密码产品有严格的管理要求，因此，SZCA 在选择加密设备时，仅参照 FIPS140-2 标准的要求，是在国家密码管理政策许可前提下的选择性适用，具体参照设备厂商提供的资料。用于此类密钥生成的密码模块须通过国家密码主管部门鉴定、认证。

6.2.2 私钥多人控制

SZCA 私钥的生成、更新、吊销、备份和恢复等操作采用多人控制机制，即采取 3 选 2 方式，将私钥的管理权限分散到 3 位密钥管理员中，至少在其中 2 人在场并许可的情况下，插入管理员卡并输入 PIN 码，才能对私钥进行操作。

6.2.3 私钥托管

对于 CA 密钥 SZCA 无托管业务。

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，系统初始化生成时进行的 CA 私钥备份。

SZCA 对 CA 的私钥进行备份。订户的签名私钥由订户产生，建议定期自行备份，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

私钥到期后，SZCA 在 10 天内完成归档操作。私钥归档保存至少 7 年。

6.2.6 私钥导入、导出密码模块

ZCA 不提供订户私钥从硬件密码模块中导出的方法，也不允许如此操作。对于存放在软件密码模块中的私钥，如果订户愿意并且自行承担相关风险，订户可自主选择导入导出的方式，操作时需要采用口令保护等授权访问控制措施。

6.2.7 私钥存储于密码模块

CA 系统的密码设备采用国家密码管理局批准和许可的服务器密码机，硬件密码模块至少符合 FIPS 140-2 三级标准或同等级安全水平，私钥的数据存储在服务器密码机硬件中，在整个生命周期都不会明文出现在硬件密码机之外。

订户的私钥存储在符合国家密码管理规定的 USB Key 介质或文件证书中，所有在 USB Key 中存储的私钥，都以密文的形式保存。对于使用软件密码模块生成的私钥，最好在硬件密码模块中存储和使用，订户也可以自主选择使用有安全保护措施的特定软件密码模块。

用于安全存储代码签名证书订户私钥的硬件密码模块至少符合 FIPS 140-2 二级标准或同等级安全水平。

6.2.8 激活私钥的方法

密钥管理员使用自己的管理员卡登录服务器密码机，进行激活私钥的操作，需要 2 名管理员同时在场。

对于存放在诸如 USB Key、加密卡、加密机或者其他形式的硬件密码模块中的订户私钥，订户可以通过口令、IC 卡等方式进一步保护。当订户计算机上安装了相应的驱动后，将 USB Key、IC 卡等插入相应设备中，输入保护口令，则私钥被激活。对于存放在订户计算机软件

密码模块中的私钥，订户应该采用合理的措施从物理上保护计算机，以防止在没有得到用户授权的情况下，其他人员使用订户的计算机和相关私钥。如果存放在软件密码模块中的私钥没有口令保护，那么软件密码模块的加载意味着私钥的激活。如果使用口令保护私钥，软件密码模块加载后，还需要输入口令才能激活私钥。

6.2.9 解除私钥激活状态的方法

密钥管理员使用含有自己的管理员卡登录服务器密码机，进行解除私钥的操作，需要 2 名管理员同时在场。

一旦私钥被激活，除非这种状态被解除，私钥总是处于活动状态。在某些私钥的使用当中，私钥每次被激活，只能进行一次操作，如果需要进行第二次操作，需要再次进行激活。

SZCA 解除私钥激活状态的方式包括退出登陆状态、切断电源、将硬件密码模块移开、注销用户或系统等。未经授权的任何人员，绝不可以进行相关操作。

订户解除私钥激活状态由其自行决定，当每次操作后注销计算机，或者把硬件密码模块从读卡器中取出，切断电源时，私钥就被解除。

6.2.10 销毁私钥的方法

如果私钥不再被使用，或者与私钥相对应的公钥到期或者被吊销后，如果其处于软件加密模块内，那么该软件加密模块必须被覆盖方式清除；如果位于硬件加密模块内，那么加密设备或者 IC 卡等必须被清空为零。同时，所有用于激活私钥的 PIN 码、IC 卡等也必须被销毁或者收回。

订户的私钥不再被使用，或者与私钥相对应的公钥到期或者被吊销后，由订户决定其销毁方法，订户必须保证有效销毁其私钥，并承担有关的责任。涉及到密钥到期后保存和归档的，订户必须按照本 CPS 的规定执行。

6.2.11 密码模块的评估

SZCA 使用国家密码管理局批准和许可的密码产品。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

对系统产生的公钥数据进行定时的归档保存，对保存的公钥信息进行对称加密，确保能获取安全完整的公钥信息。公钥到期后，SZCA 定期完成归档操作。

6.3.2 证书与密钥对使用的有效期

公钥和私钥的使用期限与证书的有效期相关，但并不完全保持一致。

对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期限以外。

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

另外需注意的是无论是订户证书还是 CA 证书，证书到期后，在保证安全的情况下，允许使用原密钥对对证书进行更新。但是密钥对不能无限期使用。

对于不同的证书，其密钥对允许通过证书更新的最长使用期限如下：

1. 对于代码签名证书，其密钥对的最长允许使用期限是 39 个月，可少于 39 个月；

2. 对于 SSL 服务器证书，其密钥对的最长允许使用期限是 398 天，可少于 398 天。

6.4 激活数据

6.4.1 激活数据的产生与安装

为了保护私钥的安全，证书订户生产和安装激活数据必须保证安全可靠，从而避免私钥

被泄漏、被偷窃、被非法使用、被篡改、或者被非法授权的披露。

CA 私钥的激活数据，必须按照有关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。订户私钥的激活数据，包括用于下载证书的口令（以密码信封等形式提供）、USB Key、IC 卡的登陆口令等，都必须在安全可靠的环境下随机产生。

SZCA 产生的激活数据，包括用于下载证书的口令（（以密码信封等形式提供）、USB Key、IC 卡的登陆口令等，都是在安全可靠的环境下随机产生。这些激活数据，都是通过安全可靠的方式，例如离线当面递交、邮政专递等方式交给订户。对于非一次性使用的激活数据，SZCA 建议用户自行进行修改。

所有的保护口令都应该是不容易被猜到的，应该遵循以下几个原则：

（1） 至少 8 位字符；

（2） 至少包含一个小写字母；

（3） 不能包含很多相同的字符；

（4） 不能和操作员的名字相同；

（5） 不能使用生日、电话等数字；

（6） 用户名信息中的较长的子字符串。

6.4.2 激活数据的保护

对于 CA 私钥的激活数据，必须将激活数据按照可靠的方式分割后由不同的可信人员掌管，而且掌管人员必须符合职责分割的要求。

订户的激活数据必须在安全可靠的环境下产生，必须进行妥善保管，或者记住以后进行销毁，不可被他人所获悉。如果证书订户使用口令或 PIN 码保护私钥匙，订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书订户使用生物特征保护私钥，订户也应注意防止其生物特征被人非法窃取。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

当私钥的激活数据进行传送时，应保护他们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

当私钥的激活数据不需要时应该销毁，并保护它们在此过程中免于丢偷窃、泄露或非授权使用，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或者全部，比如记录有口令的在纸页必须粉碎。

考虑到安全因素，对于申请证书的订户激活数据的生命周期，规定如下：

（1）订户用于申请证书的口令，申请成功后失效。

（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 个月后应要进行修改。

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 系统的信息安全管理，按照国标《证书认证系统密码及其相关安全技术规范》、工业和信息化部公布的《电子认证服务管理办法》，参照 ISO17799 信息安全标准规范以及其他相关的信息安全标准，制定出全面、完善的安全管理策略和制度，在运营中予以实施、审查和记录。主要的安全技术和控制措施包括：身份识别和验证、逻辑访问控制、物理访问控制、人员职责分权管理、网络访问控制等。

实行严格的双因素验证机制，为每位拥有系统（包括 CA 系统、RA 系统）访问权限的人员分配唯一的账户，账户的访问权限限制为执行工作职责要求的最小权限。访问时同时采用用户名、口令以及数字证书双因素登录方式。

通过严格的安全控制手段，确保 CA 软件和数据文件的系统是安全可信的系统，不会受到未经授权的访问。

核心系统必须与其他系统物理分离，生产系统与其他系统逻辑隔离。这种分离可以阻止除指定的应用程序外对网络的访问。使用防火墙阻止从内网和外网入侵生产系统网络，限制访问生产系统的活动。只有 CA 系统操作与管理组中的、有必要工作需要、访问系统的可信人员可以通过口令访问 CA 数据库。

6.5.2 计算机安全评估

SZCA 根据法律法规和主管部门的规定，按照国家计算机安全等级的要求，实现安全等级制度。

SZCA 的认证系统，通过了国家密码管理局的安全性审查。

SZCA 的认证系统、计算机及网络安全，每年由国家密码管理局主管部门对认证系统、计算机、网络安全进行年度评估审查，并根据相关专家及领导意见，对认证系统及系统安全进行升级改造。

6.6 生命周期技术控制

6.6.1 系统开发控制

SZCA 的软件设计和开发过程遵循以下原则：

（1） 制定公司内部的升级变更申请制度，并要求工作人员严格按照流程执行；

（2） 制定公司内部的采购流程及管理制度；

（3） 开发程序必须在开发环境进行严格测试成功后，再申请部署于生产环境；

（4） 变更部署前进行有效的在线备份；

（5） 第三方验证和审查；

（6） 安全风险分析和可靠性设计。

同时，SZCA 的软件开发操作规范，参考 CMMI 的标准，执行相关的规划和开发控制。

6.6.2 安全管理控制

SZCA 认证系统的信息安全管理，严格遵循国家密码管理局的有关运行管理规范进行操作。

SZCA 认证系统的使用具有严格的控制措施，所有的系统都经过严格的测试验证后才进行安全和使用，任何修改和升级会记录在案并进行版本控制、功能测试和记录。SZCA 还对认证系统进行定期和不定期的检查和测试。

SZCA 采用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。

硬件设备由采购到接收时，会进行安全性的检查，用来识别设备是否被入侵，是否存在安全漏洞等。加密设备的采购和安装具备在更加严格的安全控制机制下，进行设备的检验、安装和验收。

SZCA 认证系统所有的软硬件设备升级以后，废旧设备在进行处理时，首先必须确认其是否有影响安全的信息存在。

6.6.3 生命期的安全控制

SZCA 认证系统的软硬件设备具备可持续性的升级计划，其中包括了对软、硬件生命周期的安排。

6.7 网络安全控制

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。

为了确保网络安全，SZCA 认证业务系统安装部署了入侵检测、安全审计、防毒防范和网管系统，并且及时更新防火墙、入侵监测、安全审计、防病毒和网管系统的版本，以尽可能的降低来自于网络的风险。

6.8 时间戳

认证系统的各种系统日志、操作日志都有采用国家授时中心的标准时间。这些时间标识不需要采用基于密码的数字时间戳技术。

7. 证书、证书吊销列表和在线证书状态协议

7.1 证书

SZCA 使用的详细证书格式符合国家相关标准要求，是 ITU-T 推荐的一个国际标准 ITU-T X.509v3（1997）：信息技术-开放系统互连-目录：认证框架（1997 年 6 月）标准和 RFC 5280：Internet X.509 公钥基础设施证书和 CRL 结构（2008 年 5 月）。

7.1.1 版本号

SZCA 签发的证书符合 X.509 V3 版证书格式，版本信息存放在证书版本格式栏内。

7.1.2 证书扩展项

SZCA 除了使用 X.509 V3 版证书标准项和标准扩展项以外，还使用了自定义扩展项。

- 证书标准项

1.证书版本号(Version)

指明 X.509 证书的格式版本，值为 V3。

2.证书序列号（Serial Number）

即由 SZCA 通过 CSPRNG 生成大于 0 且长度为 64 位的非序列性的证书序列号，是证书唯一的数字型标识符。

3.签名算法标识符（Signature）

指定由 SZCA 签发证书时所使用的签名算法。

4.签发机构名（Issuer）

用来标识签发证书的 CA 的 X.500 DN 名字。即 SZCA 各个属性，包括国家、省、市、机构、单位部门、和通用名。例如：

CN = SZCA EV SSL CA

OU = IT Dept

O = SZCA

L = Shenzhen

S = Guangdong

C = CN

5.证书有效期（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。

6.证书主体（Subject）

指定证书持有者的 X.500 的甄别名。包括国家、省、市、机构、单位部门和通用名，还可包含 email 地址等个人信息等。

SSL 证书，通用名应包含与服务器关联的用户所拥有或控制，且为主体别名扩展项之一的的域名或 IP 地址；EV SSL 证书的通用名只能为域名，不能为 IP 地址，不能为通配符。

7.证书持有者公开密钥信息（subject Public Key Info）

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。

- 证书扩展项

1.颁发机构密钥标识符（authorityKeyIdentifier）

颁发机构密钥标识符扩展提供了一种方式，以识别与证书签名私钥对应的公钥。当颁发者由于有多个密钥共存或由于发生变化而具有多个签名密钥时使用该扩展。

2.主体密钥标识符（subjectKeyIdentifier）

本项提供一种识别包含有一个特定公钥的证书的方法。此扩展标识了被认证的公开密钥。它能够区分同一主体使用的不同密钥（例如，当密钥更新发生时）。

3.密钥用法 (key usage)

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。

4.CRL 发布点

由 SZCA 指定的 CRL 发布点。

5.主题替换名/主题别名

非关键项，包括证书用户所拥有、控制的与其服务器关联的所有域名或 IP 地址。EV 证书该项不能包含通配符或 IP 地址。

6.机构信息访问

包含证书颁发机构 SZCA 的 OCSP 响应的 HTTP URL（accessMethod = 1.3.6.1.5.5.7.48.1），及颁发证书的 OCSP 的响应的 HTTP URL（accessMethod = 1.3.6.1.5.5.7.48.2）。通过访问该地址，能够获取 SZCA 的 CA 证书及其颁发的用户证书的状态信息。

- 自定义扩展项

7.1.3 算法对象标识符

SZCA 签发的证书中，密码算法的标识符为 sha256RSA、 SM2、和 SM3。

7.1.4 名称形式

SZCA 签发的证书名称形式的格式和内容符合 X.501 Distinguished Name(DN)的甄别名格式。

7.1.5 名称限制

未规定

7.1.6 证书策略对象标识符

未规定

7.1.7 策略限制扩展项的用法

未规定

7.1.8 策略限定符的语法和语义

未规定

7.1.9 关键证书策略扩展项的处理规则

未规定

7.2 证书吊销列表

SZCA 定期签发 CRL（证书吊销列表），供用户查询使用。SZCA 签发的 CRL 遵循 RFC5280 标准。

7.2.1 版本

SZCA 的证书吊销列表采用 X.509 v2 版的证书格式。

7.2.2 CRL 项与 CRL 条目扩展项

SZCA 的证书吊销列表（CRL）是一个带有时间戳并且经过数字签名的已吊销证书的列表。CRL 的签发者是 CA，SZCA 通过发布 CRL 提供它所签发的数字证书的状态信息。

（1）CRL 的版本号：用来指定 CRL 的版本信息，SZCA 采用的是同 X.509 V3 证书对应的 CRL V2 版本。

（2）签名算法：SZCA 采用 sha256RSA、SM2withSM3 签名算法。

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

（4）生效时间：指定一个日期/时间值，用以表明本 CRL 发布的时间。

（5）更新时间：指定一个日期/时间值，用以表明下一次 CRL 将要发布的时间（本标准强制使用该域）。

（6）吊销证书列表：指定已经吊销的证书列表。本列表中含有证书的序列号和证书被吊销的日期和时间。

（7）颁发机构密钥标识符（Issuer Unique Identifier）：本项标识用来验证在 CRL 上签名的公开密钥。它能辨别同一 CA 使用的不同密钥。

7.3 在线证书状态协议

SZCA 采用 IETF PKIX 工作组开发的一个在线证书状态协议 (Online Certificate Status Protocol，OCSP，RFC6960)，该协议定义了一种标准的请求和响应信息格式以确认证书是否被吊销了。在 SZCA 官方网站下载 OCSP 查询客户端并按照 SZCA 官方网站发布的 OCSP 操作说明进行配置，即可使用 SZCA 的在线证书状态查询服务。SZCA 签发的 OCSP Version 为 v1 版。

SZCA 签发的 OCSP 响应至少包含以下所述的 OCSP 机构基本域和内容：

（1） Version：客户端使用的 OCSP 协议的版本号；SZCA 的在线证书状态协议为 v1 版；

（2） signatureAlgorithm：签发 OCSP 的算法；

（3） responderID：签发 OCSP 的实体。签发者公钥的 SHA1 数据摘要值和证书甄别名；

（4） producedAt：OCSP 响应生成的日期和时间；

（5） Signature：OCSP 响应消息的数字签名；

（6） Nonce(一次性随机数)：在状态请求消息中的每一个 requestExtensions 变量和响应消息中的 responseExtension 变量中包含一次性随机数，防止重放攻击；

（7） 证书状态：证书的最新状态，包括有效、吊销和未知。

7.3.1 OCSP 请求和响应处理

一个 OCSP 请求包含以下数据：协议版本、服务要求、目标证书标识和可选的扩展项等。

在接受一个请求之后，OCSP 服务端响应时进行如下检测：

SZCA 的 OCSP 响应符合 RFC6960 标准。客户通过 http 协议访问 SZCA 的 OCSP 服务，SZCA 会对查询请求进行检查，OCSP 签名证书包括 RFC6960 定义的 id-pkix-ocsp-nocheck 的扩展项。

- 信息正确格式化
- 响应服务器被配置提供请求服务
- 请求包含了响应服务器需要的信息，如果任何一个先决条件没有满足，那么 OCSP 服务端将产生一个错误信息；否则的话，返回一个确定的回复

所有确定的回复都由证书签发者密钥进行数字签名，主要回复状态包括：证书有效、已吊销、未知。回复信息由以下部分组成：

- 回复语法的版本
- 响应服务器名称
- 对请求端证书的回复
- 可选扩展
- 签名算法对象标识符号

- 对回复信息散列后的签名

如果出错，OCSP 服务器会返回一个出错信息，这些错误信息没有 SZCA 证书签发者密钥的签名。出错信息主要包括：

- 未正确格式化的请求（malformedRequest）
- 内部错误（internalError）
- 请稍后再试（trylater）
- 需要签名（sigRequired）
- 未授权（unauthorized)

8.认证机构审计与其它评估

8.1 评估的频率或情形

SZCA 可以针对运营及服务开展以下两种评估：

（1）外部评估

SZCA 聘请独立第三方机构进行 CPS 执行情况的审查。

签发 EV 证书的 CA 机构应按照以下任一方案接受审计：

（i）对 CA 机构和 Web trust EV 证书方案进行审计的 Web Trust 方案；

（ii）对 EVCP 进行 ETSI TS 102 042 审计，或

（iii）对 EVCP 的策略进行 ETSI EN 319 411-1 审计。

（2）内部评估

SZCA 运营安全管理小组，按照国家现行有效的认证行业法律法规、本 CPS 及其他 SZCA 内部的管理规章，定期进行内部审查，并且按照机构内部规范的评估方法和程序进行。对 CA 中心及其注册机构进行评估，频率通常为每年一次，特殊情况除外。

CA 应每年在内部审核每个委托第三方遵守这些要求的情况。

在技术受限的从属 CA 颁发证书期间，签署从属 CA 的 CA 应监控对 CA 的证书策略和从属 CA 的证书实践声明的遵守情况。至少每季度一次，对于随机选择的一类证书中较大一个的样本或下级 CA 颁发的证书的至少百分之三，在上一次审计样本采取后立即开始的期间内，CA 应确保所有符合适用的 CP。

在签发 EV 证书的期间，CA 机构应自上次采样完成后开始签发的证书中随机抽取至少 3%比例进行自我审查，以此严格管控服务质量。对由 RA 按照《EV 证书签发管理指南》第 11.13 节要求履行交叉验证和合理注意义务的所有 EV 证书，CA 机构应自上次采样完成后开始签发的证书中随机抽取至少 6%比例进行自我审查，以此严格管控服务质量。

8.2 评估者的资质

CA 的审核应由合格审核员执行。合格审计师是指自然人，法人实体或自然人或法人团体，他们共同拥有以下资格和技能：

（1） 独立于被审计主体;

（2） 能够进行符合合格审计计划中规定标准的审计（见第 8.1 节）;

（3） 聘用熟练掌握公钥基础设施技术，信息安全工具和技术，信息技术和安全审计以及第三方认证功能的人员;

（4） （对于按照 WebTrust 标准进行的审核），由 WebTrust 许可;

（5） 受法律，政府法规或职业道德规范的约束;和

（6） 除内部政府审计机构外，维持专业责任/错误责任保险，保单限额至少为 100 万美元。

8.3 评估者与被评估者的关系

第三方评估者与 SZCA 之间没有任何的业务、财务往来，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。

SZCA 的内部评估者，与被评估的对象之间，也应无直接的任何足以影响评估客观性的利害关系，评估者应以独立、公正、客观的态度对被评估的对象进行评估。

8.4 评估内容

CA 应按照以下方案之一进行审核：

1. WebTrust for CAs v2.0 或更高版本和 WebTrust for CAs SSL Baseline with Network Security v2.2 或更高版本;

2.如果其证书政策要求政府 CA 使用不同的内部审计计划，则可以使用此类计划，前提

是审计要么（a）包含上述计划之一的所有要求，要么（b）包含可供公众审查的可比标准。

无论选择哪种方案，都必须纳入定期监测和/或问责程序，以确保其审计继续按照计划的要求进行。

审核必须由合格审核员进行，如第 8.2 节所述。

对于非企业 RA 的授权第三方，CA 应获得根据审核标准颁发的审核报告，该审核标准是第 8.1 节中所接受的审核方案的基础，该审核报告提供了对委托第三方的绩效是否符合 委托第三方的执业声明或 CA 的证书政策和/或证书业务声明。如果意见是委托第三方不遵守，则 CA 应不允许授权第三方继续履行授权职能。

授权第三方的审核期限不得超过一年（理想情况下与 CA 的审核一致）。 但是，如果 CA 或委托第三方在多年内完成对政府实体和审计计划的运营，控制或监督，那么年度审计必须至少涵盖每年需要审计的核心控制。 通过这种方案加上允许不那么频繁地进行的所有非核心控制的部分，但在任何情况下，任何非核心控制都不得少于每三年审核一次。

8.5 对问题与不足采取的措施

针对行业主管部门工信部及其认可的第三方审计机构的评估，SZCA 将根据评估结果检查缺失和不足，提交纠正改进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。

8.6 评估结果的传达与发布

审计报告应明确声明它涵盖了发布所有证书的相关系统和流程，这些证书断言第 7.1.6.1 节中列出的一个或多个策略标识符。 CA 应公开审计报告。 CA 不需要公开任何不影响整体审计意见的一般审计结果。 对于政府和商业 CA，CA 应该在审计期结束后的三个月内公布

审计报告。 如果延迟超过三个月，并且如果应用软件供应商提出要求，CA 应提供由合格审核员签署的解释性信函。

9. 法律责任和其它业务条款

9.1 费用

9.1.1 证书签发与更新费用

根据市场、物价部门及行业主管部门的规定，SZCA 将收取合理的证书及相关服务费用。在订户向 SZCA 提出各种证书申请要求时，SZCA 提前告知订户 SZCA 证书签发等各种证书管理行为的收费项目、标准与方式。

订户须按照约定向 SZCA 支付证书费用，否则即使证书已签发或订户已开始使用证书，SZCA 有权吊销该证书。

9.1.2 证书查询费用

SZCA 暂不收取此项收费，但保留对此项服务收费的权利。

9.1.3 证书状态信息查询费用

SZCA 暂不收取此项收费，但保留对此项服务收费的权利。

9.1.4 其它服务费用

SZCA 保留收取其他服务费的权利。

9.1.5 退款策略

如 SZCA 违背本 CPS 所规定的责任与义务，订户可以要求退款。否则，SZCA 对订户收取的费用均不退还。

订户应当提供符合 SZCA 要求的完整、真实、准确的证书申请信息，否则 SZCA 对此造成

的损失和后果不承担任何责任。

9.2 财务责任

9.2.1 保险范围

SZCA 根据业务发展情况决定其投保策略，目前暂无。

9.2.2 其他资产

SZCA 确保具有足够的财务实力来维持其正常经营并保证相应义务的履行，并合理地承担对订户及对依赖方的责任。

9.2.3 对最终实体的保险与担保

目前，SZCA 仅根据《电子签名法》的规定，对于由于 SZCA 的原因给订户造成的直接损失予以限额赔偿。根据订户所使用的证书的类型，赔付的额度有所不同，具体的赔付标准同本 CPS 9.8。在适当的情况下，SZCA 将排除安排采购适当的保险或作出符合监管部门要求其他方式的赔偿安排（例如赔偿保证存款金）。

9.3 业务信息保密

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 授权的注册机构之间、SZCA 及其授权的注册机构与订户之间、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）与订户证书公钥配对的私钥；

（3）SZCA 的审计日志及其他审计文件等；

（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非公开信息等。

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

非保密信息包括以下内容：

（1）SZCA 公布或提供的与证书申请及使用有关的指导说明性文件、及 CPS 等；

（2）订户证书中包括的相关公开信息，如订户公钥等；

（3）证书状态及吊销列表信息；

（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商业性使用，对于利用非保密信息的第三方主体，SZCA 和信息的所有人保留追究其法律责任的权利。

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、依赖方以及与认证业务相关的参与方等，均有义务按照本 CPS 的规定，承担相应的保护保密信息的责任。

SZCA 制定员工信息保密管理规范，并与员工签订保密协议，且会对所有员工进行信息保密的相关培训，规范员工访问、获取及使用上述保密信息的行为，保障 SZCA 的证书管理工作严格符合信息保密的相关法律规定要求。

当机密信息的所有者要求 SZCA 公开或披露其保密信息，SZCA 按在法律法规规定和订户

的要求进行公开；同时，机密信息持有者应向 SZCA 提供书面授权文件，说明授权公开信息意愿，公开的方式、内容和范围。如发生与该获授权的保密信息披露行为相关或由此引发的任何第三方的损失赔偿，SZCA 不承担责任，由订户负责赔偿所有损失，包括 SZCA 的损失在内。

当 SZCA 按照法律法规、司法机关裁判文书的要求，必须披露具有保密性质的信息时，SZCA 可以向执法部门披露相关的保密信息。这种披露不视为违反保密的要求和义务。

9.4 个人信息保密

9.4.1 隐私保护方案

SZCA 尊重所有订户的隐私。SZCA 的隐私保护策略，按照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。一旦出台新的与保护隐私相关的法律，本 CPS 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，就意味着表示已经同意接受 SZCA 有关隐私保护的制度。

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及证书状态信息外，该订户的基本信息和身份认证资料，非经订户同意，或法律法规作出规定，及相关司法机关裁判要求，绝对不会任意对外公开。

9.4.3 非隐私的信息

订户的公钥证书内包括的信息，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、依赖方以及与认证业务相关的参与方等，都有义务按照本 CPS 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、或者司法机关在合法程序的要求下，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。这种披露不被视为违反隐私保护义务。与披露行为相关的或由此引发的损失，SZCA 无须为此承担任何责任。

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、管理证书和服务订户的目的。在使用这些信息时，无论是否涉及到隐私，SZCA 都没有告知订户的义务，也无需得到订户的同意。

SZCA 在任何法律法规规定或者司法机关、行政执法机关等有权机关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订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，事前需告知订户并征得其书面同意，获得经订户签章的书面授权文书。

9.4.6 依司法或行政程序进行信息披露

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第三方主体：

（1）订户书面授权同意 SZCA 披露的；

（2）司法机关，如公安机关、国家安全机关、检察院、法院等因案件侦查需要，向 SZCA 提出要求的；

（3）获得司法机关授权的诉讼案件当事人及其诉讼代理人、律师等，向 SZCA 提出要求

的；

（4）法院为执行有关证书的裁决、或仲裁机构作出的申请法院执行的裁决，向 SZCA 提出书面申请；

（5）国家行政执法机关为合法行政管理的需要，向 SZCA 要求的。

证书订户因自身的原因需要，向 SZCA 提出隐私信息披露申请的，SZCA 将根据书面授权文件或相关协议对相关信息进行披露。经授权同意进行的披露行为，如发生任何与披露相关的或由于披露该隐私信息所造成的任何损失、及不利影响，SZCA 一律不承担任何责任。

无论是行政机关、司法机关还是第三人，要求 SZCA 进行订户信息披露的，应持有法定机构出具的合法证明文件，且按照法定程序提出调取申请。

SZCA 依法进行的信息披露，如发生任何与披露相关的或由于披露该隐私信息所造成的任何损失、及不利影响，SZCA 一律不承担任何责任。

9.4.7 其他信息披露情形

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、文档、数据的独占的知识产权，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。

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，上述知识产权包括但不限于相关的 SZCA 的规范性文件、CP/CPS、技术支持文件和使用手册等各种数据、信息、资料。SZCA 的其他电子认证服务机构在征得 SZCA 的授权同意后，可以使用相关的文件和手册。

在没有 SZCA 事先书面同意的情况下，任何使用者在任何证书到期、作废或效力终止后，不能商业性地使用任何 SZCA 使用的名称、商标、或可能与之相混淆的名称、商标或商务称

号。

9.6 陈述与担保

对于证书的订户、SZCA 及其授权注册机构、依赖方等，除非 SZCA 在相关服务协议中有特别约定，否则，当本 CPS 的规定与其它 SZCA 制订的规范性文件规定相冲突，优先适用本 CPS；协议内容与本 CPS 规定不一致的，以协议内容为准；对协议中未约定的内容，按本 CPS 的有关规定执行。

9.6.1 电子认证服务机构的陈述与担保

通过颁发证书，SZCA 将下述列出的证书保证提供给以下证书受益人：

1.作为订户协议的一方或证书使用协议的订户；

2.所有与根 CA 签订合同，将根证书包含在其分发的软件中的应用软件供应商；和

3.所有合理依赖有效证书的依赖方。

SZCA 向证书受益人声明并保证，在证书有效期间，SZCA 在颁发和管理 SSL 证书时遵守了 CA/B 论坛制定的 SSL 证书要求、本 CPS、CP(如有)。

SZCA 对于签发的证书，提供包括但不限于以下特别保证：

- 订户有权使用证书中所提述的域名或 IP。

SZCA 在签发证书时，已采取并遵循符合本 CPS 、CP（如有）规定的域名使用权验证程序，对申请人有权使用或控制证书中的证书主体项和主体替换名称扩展项中的域名或 IP，进行了适当的验证（或仅含域名的情况下，获得域名权利人有关使用、控制域名的授权）。

- 订户授权签发证书。

SZCA 在签发证书时，已采取并遵循符合本 CPS 、CP（如有）规定的证书授权程序，对订户的证书（申请）的意愿、授权，及证书申请代理人/代表人代表订户申请证书的授权权限等事项进行了适当的验证。

- 证书中信息的准确性和非误导性。

SZCA 在签发证书时，已采取并遵循符合本 CPS 、CP（如有）规定的信息核验程序，验证证书中所含的全部信息(主体的机构部门名称属性项除外)的准确性；并降低证书主体的机构

部门名称项令人误解的可能性。

- 订户/申请人身份的真实

如证书中包含订户/证书主体的身份信息，SZCA 应采取第 3.2 节规定的程序，对订户的身份进行核验和确认。

对于 EV 证书，在证书 SZCA 将与注册所在地的注册管理机关核实该机构主体在注册地是真实合法存在的机构；且证书中该主体的法定名称，与注册管理机关官方注册文件中的机构名称匹配一致。

- 签署订户协议

如订户和 SZCA 无从属关系，应依 CA/B 论坛 SSL 证书要求、本 CPS 、CP（如有）签署符合的合法有效的订户协议；如 SZCA 与订户属同一实体或有从属关系，证书申请代理人应认可证书使用协议。

- 证书状态服务

SZCA 对所有未到期的证书，向公众提供 24X7 可用的证书当前状态信息服务。

- 吊销服务

对因本 CPS 规定的任何证书吊销事由出现时，SZCA 及时吊销证书。

针对 EV SSL 证书，在证书有效期内，SZCA 遵循 CA/B 论坛有关的证书要求、本 CPS 及 CP*如有），验证证书中所含信息的准确性，签发和管理 EV 证书。

9.6.1.1 SZCA 对于自身服务的一般性陈述

（1） 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；

（2） 建立符合国家有关法律规定、国家标准、行业标准的信息基础设施提供认证服务；

（3） 建立和执行符合国家相关政策的规定的安全机制，保证 SZCA 本身的签名私钥得到安全的存放和保护；

（4） 所有和认证业务相关的活动都符合国家的法律法规和主管部门的规定、CPS、CP 及其他机构内部的规章制度；

（5） SZCA 及其授权证书注册机构，是客观中立的第三方证书服务机构。

SZCA 不是证书订户或依赖方任意一方的代理人、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。证书订户和依赖方无权以合同形式或其它方法要求 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。

(1) SZCA 通过公开发布证书，向所有查询或合理信任 SZCA 信息库及其中证书信息的人承诺：发证机构已按有关法律法规及 CP、CPS 的要求向订户签发证书，并且订户已经按照本 CPS 中的规定接受了该证书。

9.6.1.2 SZCA 对订户的陈述与担保

除非 SZCA 与订户另有约定，SZCA 须对证书订户承担包括但不限于以下的担保责任，：

（1）证书中没有 SZCA 所知的或源于 SZCA 的错误陈述；

（2）生成证书时，不因 SZCA 的失误而导致证书中的信息与 SZCA 所收到的信息不一致；

（3）签发给订户的证书符合本 CPS 及其 CP 的实质性要求；

（4）将按本 CPS 及其 CP 及相关电子认证业务规则的规定，及时吊销证书，并将证书的状态信息及时发布到 CRL 及 OCSP 上；

（5）将作出合理努力向订户通报任何已知的、或将在根本上影响证书有效性和可靠性的事件。

9.6.1.3 SZCA 对依赖方的陈述与担保

SZCA 须对依赖方（按照本证书策略及相关电子认证业务规则合理地依赖签名（该签名可通过证书中所含的公钥验证）的人）承担包括但不限于以下责任：

（1）除未经验证的订户信息外，证书中或证书指向的相关信息都是准确的；

具体来说，有关证书内容及状态信息，SZCA 可向依赖方提供以下保证：

第一，证书持有人、使用人的合法存在性；

第二，证书订户的身份经过有效识别；

第三，证书中关于证书订户、持有人信息的准确性；

第四，证书状态 7*24 小时可查询；

第五，CA 根据 CPS 规则，废止不符合生效条件的证书。

（2）完全遵照本 CPS 及其 CP 的规定签发证书；

（3）通过公开发布证书，向所有合理依赖证书中信息的依赖方证明：发证机构已向订户签发证书，并且订户已按照本 CPS 及其 CP 的规定接受了该证书；

（4）及时吊销证书，并更新证书的状态信息。

上述陈述仅仅是为保证订户和依赖方的利益，而不是用于使任何其它主体受益或使其它主体承受不应承担的不合理的责任。

9.6.2 注册机构的陈述与担保

经 SZCA 合法程序获得授权的注册机构 RA 保证：

（1）遵循本 CPS、CP 和 SZCA 的授权协议、业务管理规范及其它 SZCA 的认证业务标准和流程，依法受理并处理证书申请；

1) 根据证书申请材料，采取法律法规及本 CPS 规定的合理措施，对订户的身份进行鉴别与验证。如注册机构对订户的证书申请材料审查没有通过，注册机构有向订户进行告知的义务；

2) 注册机构应在规定的时间内完成证书申请处理；

3) 注册机构有义务通知订户阅读 SZCA 发布的 CP、CPS 以及其它相关规定，在订户完全知晓并同意 CP、CPS 和证书服务协议内容的前提下，为订户办理数字证书；

4) 注册机构应使订户明确地知道关于使用第三方数字证书的法律意义、数字证书的功能、使用范围、使用方式、密钥管理以及丢失数字证书的后果和处理措施、法律责任限制，尽到对订户安全提示的义务；

5) 注册机构须对订户的信息及与认证相关的信息妥善保存，并于适当的时间转交 SZCA 归档。

（2）遵循 SZCA 制订的业务处理规范、业务运营规范、系统运作规范及其他运营服务管理规范等；

（3）依据 SZCA 的授权设置各类下级证书服务受理机构，包括 RA、LRA 等，并按照行业法律及 SZCA 的各种运营服务管理规范，对其进行监督和管理等；

（4）依据本 CPS 的规定，确保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 必须能够对证书服务相关的全部数据资料进行备份；

（5）按照 SZCA 的要求，保证其与下级证书服务机构间的信息传输安全。并且 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。

（6） 接受 SZCA 根据本 CPS 和授权协议对 RA 进行管理，包括接受服务资质审核和规范执行检查，根据相关协议内容配合 SZCA 需要的电子认证业务合规性审计。 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。

（7）为证书申请者提供必要的服务及技术咨询。

9.6.3 订户的陈述与担保

在签发证书前，SZCA 将为 SZCA 本身及其他证书受益人的利益，与订户签订合法有效订户协议或证书使用协议。SZCA 将采取适当程序确保协议的效力。单个订户协议可用于多张证书申请；也可对不同的证书申请分别签署对应的订户协议，具体情况由 SZCA 酌情决定。订户协议也可采取电子形式，通过“点击”完成签署，如 SZCA 认定该电子协议在法律上有效可执行。

订户一旦接受 SZCA 及其授权注册机构签发的证书，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，则订户需向 SZCA 及所有合理信赖证书中所含信息的依赖方，做出如下承诺和保证：

1.信息的准确性：订户有义务并保证，无论是证书申请还是经 CA 为颁发证书要求的，

始终向 CA 提供真实、准确、完整的申请材料、信息，包括申请过程中所作的陈述、声明与保证，是可供 SZCA 及相关依赖方检查和核实；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，订户和代理人两者负有无限连带责任。 作为订户，有责任就因申请代理人的疏忽所作的任何不实陈述、错误陈述或遗漏，及时通知通知 SZCA 或其下属发证机构，申请吊销证书或重新申请证书或申请证书更新（包含密钥更新）。

2.私钥保护：申请人有义务和保证采取一切合理措施，采用可靠的方式生成密钥对，采取安全措施保证私钥的安全存储，保证私钥及其存储介质与设备的保密性，使用可靠的系统，以确保控制、保密和妥善保护与包含在所请求的证书中公钥相对应的私钥（以及任何相关的激活数据或设备，例如密码或令牌）；

3.证书的接受：订户有审核并验证证书内容的准确性的义务和保证。订户获取证书后，应先测试检查证书中所含信息是否正确，如果有失误或者遗漏，应在合理的期间内通过 SZCA 提供的联系方式通知 SZCA。如发现问题，应停止使用证书，并及时通知 SZCA；一旦接受并使用证书，即表明订户承诺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。

4.证书的使用：有义务并保证仅在证书中主体替换名称可访问的服务器上安装证书，并按照法律、CPS、及相关的用户/订户协议约定的证书使用条件和范围操作该证书的，并且对该证书的使用是按照订户本人的真实意愿，或者按照订户的委托授权用于为其处理事务。订户应保证本人对于证书私钥的控制，不得任意交于他人占有、使用或随意告知他人使用私钥的方法，否则需自行承担私钥被盗用冒用的法律责任；并且一旦发现因自身疏忽造成密钥泄露、遗失等，或发生非自身原因造成的私钥被非法破坏、篡改、非授权使用的失密情况，应立即停止证书的使用，及时通知 SZCA 及依赖方，申请对证书进行吊销操作。

5.报告和吊销：对以下内容的义务和保证：（a）如果证书中公钥相关联的订户私钥存在任何实际或可疑的误用或泄露，应立即请求吊销证书，并停止使用该证书及其相关的私钥，以及（b）如果证书中的任何信息不正确或发生变化，请立即请求吊销证书或证书变更，并停止使用证书。在订户未通知发证机构之前的期间，SZCA 及其发证机构有理由认为：订户认为上述信息都是真实的。

6.终止使用证书：有义务和必须在因密钥泄露吊销证书时，立即停止使用与证书中包含的公钥相对应的私钥。

订户只能在 SZCA 的证书处于正常状态时才可以使用该证书；当证书被吊销（包括但不限于证书到期），或者在吊销前的调查期间的任何效力未恢复正常之前，不得将证书用于任何民事活动中，禁止将证书用于从事违法犯罪活动。因为 SZCA 只未有效期内且证书状态正常的证书提供各种服务，对于效力状态异常的证书，SZCA 将通知订户暂停或终止使用该证书，并在 CRL 及 OCSP 等中更新该证书的状态效力信息。

7.响应能力：有义务在指定时间内回复 SZCA 关于密钥泄露或证书滥用的指令。

8.认可和接受：确认并接受如果申请人违反订户协议或证书使用条款或 SZCA 发现证书被用于实施犯罪活动，如网络钓鱼攻击、欺诈或恶意软件传播等，则 SZCA 有权立即吊销证书活动。

上述因订户自身原因给 SZCA 造成任何责任、损失，及任何诉讼及其产生的全部费用，订户将予以经济赔偿。

9.6.4 依赖方的陈述与担保

依赖方在信赖任何 SZCA 签发的证书时保证：

（1）熟悉所信赖所使用的类型的证书所对应的 CPS 及证书策略，了解证书的使用目的和可获得的保证，只在符合本 CPS 规定的证书应用范围内信任该证书；

（2）依赖方在信任证书前，须同意依赖方协议中的条款，并根据使用的环境和条件判断该证书是否可信任；

（3）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 获得该证书的状态，确认该证书没有被吊销；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；检查其它能够影响证书有效性的信息；

一旦由于疏忽或者其它原因未履行合理检查的义务，依赖方愿意承担因此造成的自身或

他人的损失，并且就此对 SZCA 带来的损失进行补偿。

（4）对证书的信赖行为，表明依赖方已经接受本 CPS 有关依赖方权利义务责任的所有规定，尤其是其中有关免责、限制责任及担保和义务的条款；

（5）信任证书前确认证书记载内容与信任所需的证明是一致的；

（6）依赖方须承担因未履行以上责任所产生的法律责任。

9.6.5 其它参与方的陈述与担保

所有参与 SZCA 电子认证活动的主体，均需遵守 SZCA 相应类型证书对应的 CPS 的规定。

为 SZCA 系统、计算机及网络安全、软硬件设备等提供服务或技术支持的第三方机构或主体，须承诺该服务达到正式服务协议所约定的技术标准，能支持 SZCA 提供证书服务所需要的技术和安全条件和环境。

在对订户申请进行身份鉴别与验证中，SZCA 委托的第三方机构或主体进行调查或者使用第三方的技术，第三方也应保证在考虑所有身份材料和收集的信息的基础上，能够达到准确验证鉴别身份的效果。

上述所有与 SZCA 或其授权的注册机构合作的第三方机构及其工作人员，均应对合作过程中所获取的订户、SZCA 及其他服务过程中获取的有关主体的信息进行保密，不得进行商业性的利用，也不得未经其同意向其他任何人非法披露、提供。

9.7 担保免责

除本 CPS 9.6.1 中明确承诺的外，对于意外事件、不可抗力、非因 SZCA 方原因造成的损害，SZCA 不对此承担责任。具体 SZCA 免于承担责任的情形包含但不限于以下情形：

（1）由于如 9.16.4 所列的不可抗力因素导致 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 CPS 9.6.3 之承诺时，SZCA 得以免除承担责任；

具体来说，当订户违反下列责任和义务时，由订户自行承担责任，SZCA 不予负责：

1) 订户或其证书申请代理人有意或无意提供虚假、不完整或不准确的申请信息，或者在证书申请过程中身份信息发生变化但又不告知 SZCA，故意或过失隐瞒真实情况或提供失实的信息，导致 SZCA 签发的证书内容错误；

2) 订户或依赖方没有在可靠安全的系统中使用证书；

3) 订户或依赖方没有履行妥善保管私钥的义务；

4) 订户违反证书对应的 CPS、CP 及相应的证书文件中规定或约定的证书用途规定，超出法定或约定的范围使用，或将证书用于其他限制、禁止的范围，或将证书用于从事非法活动。

（3）证书依赖方违反本 CPS 9.6.4 之承诺时，得以免除 SZCA 的责任；

（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）在订户提出证书吊销请求后，到 SZCA 实际完成吊销该证书的期间，如果该证书被用以进行非法交易，或者发生其他相关证书使用纠纷的，如果 SZCA 按照本 CPS 的规范进行有关操作，SZCA 不承担任何损害赔偿责任；

（6）SZCA 在法律许可的范围内，依据法律、法规等以及订户、依赖方的要求如实提供网络交易中电子签名验证服务，对非因验证服务导致的损失不承担责任。

9.8 有限责任

SZCA 仅为 CPS 规定的认证服务提供赔偿，且当事人提出赔偿请求，需提供相应的合法证明材料，如法院或仲裁机构的裁决文书等。但 SZCA 能证明是按照《电子签名法》、《电子认证服务管理办法》等认证服务行业法律法规，及在工信部备案的 CPS 提供服务的，则 SZCA 不具过错，无需向订户或依赖方进行赔偿或补偿。

SZCA 对订户、依赖方的损失赔偿责任，是一种限额责任。且 SZCA 只对因使用、信赖证书而产生的直接损害负责，而不承担对间接损害、利润利息损失、精神损害等的赔偿责任，及惩罚性赔偿等责任。

除非有关特定证书的生效的法院裁决或仲裁机关的裁定对赔偿金额另有规定，SZCA 及其授权的注册机构，就每份证书对于该证书关系所有参与人（包括但不限于订户、依赖方）合计的赔偿金额，限制在下述数额的范围内（单位：人民币元）：

证书类型	赔偿金额上限
DV SSL 证书	50,000 元（RMB）
OV SSL 证书	400,000 元（RMB）
EV SSL 证书	800,000 元（RMB）
EV 代码签名证书	300,000 元（RMB）

每份证书的赔偿责任均有限额，无论数字签名费用、交易损失的多少，也不考虑提出索赔请求主体人数或索赔额度。

该限额内的赔偿款项的支付，依据的是生效的支持索赔请求的法院判决书或仲裁机构的仲裁裁决。赔偿款项的赔付，按照索赔人向 SZCA 提交有效的裁判文书或裁决书的顺序进行，不论该限额赔偿在多个索赔者直接如何分配。对于限额赔偿完毕后的其他主体的赔付请求，SZCA 对于超出赔偿限额部分的赔偿请求不予赔偿。

9.9 赔偿

1. CA 机构的赔偿

订户或依赖方进行的民事活动因 SZCA 提供的认证服务而遭受的损失,如 SZCA 签发内容有误的证书或证书失误签发交付给订户外主体、或 SZCA 造成密钥失密泄露、SZCA 在订户申请资料提交不全或虚假且明知的情况下签发内容不实的证书等，SZCA 将依据本条款进行相应的赔偿。对于委托第三方的，SZCA 和受托第三方间的责任按照合同进行分配，但首先应

由 SZCA 按照本款要求对损失各方履行全部赔偿责任。

除了 CA 是政府实体的情况之外，CA 应对每个应用软件供应商进行辩护，赔偿并保护其免受此类应用软件供应商因发出的证书而遭受的任何和所有索赔、损害和损失。但是，这未规定于此类应用软件供应商因 CA 颁发的证书而遭受的任何索赔、损害或损失，此类索赔、损坏或损失直接由此类应用软件供应商的软件显示为不值得信任的证书仍然有效或显示为可信：（1）已过期的证书，或（2）已被吊销的证书（但仅限于当前可从 CA 在线获取吊销状态的情况，以及应用程序软件未能检查此状态或忽略吊销状态的指示）。

2. 订户的赔偿责任

有下列情形之一的，订户应承担相应的损失赔偿责任：

（1）订户申请注册证书时，故意、过失提供不真实、不完整、不准确的申请材料，造成 SZCA、注册机构或者第三者遭受损害的；

（2）证书信息发生变更时未停止证书使用并及时通知 SZCA 及其授权的证书服务机构；

（3）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、遗失而没有通知依赖方、SZCA 及其授权的证书服务机构；

（4）没有对证书私钥采取有效的安全保护措施或在不安全的系统使用证书，造成私钥丢失、被盗或者泄露等；

（5）将私钥及证书不当交付他人使用，造成 SZCA、依赖方遭受损害的；

（6）将证书用于非本 CPS 规定的其它用途或业务范围的，或者将证书用于法律法规禁止的违法犯罪活动；

（7）证书被吊销（包含但不限于证书到期）期间仍然使用证书；

（8）其他订户使用证书违反本 CPS 及相关操作规范的情形。

在订户提出证书吊销请求后，到 SZCA 实际完成吊销该证书的期间，如果该证书被用以进行非法交易，或者发生其他相关证书使用纠纷的，如果 SZCA 按照本 CPS 的规范进行有关操作，相关证书纠纷产生的法律责任由订户自行承担。

SZCA 与订户签署的协议另有赔偿规定的，从其规定。

（3） 依赖方的赔偿责任

用户使用或信赖证书时，未能依照本 CPS 4.1.1 和 4.5.2 中有关依赖方责任和义务等规范履行合理审核、注意义务，导致 SZCA 或第三方遭受损害的，依赖方将对上述主体的损失进行赔偿。

9.10 有效期与终止

9.10.1 有效期限

本 CPS 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，最新版本的 CPS 请访问 SZCA 网站下载获取，对具体个人不做另行通知，新发布的 CPS 自动取代废止旧 CPS。

9.10.2 终止

本 CPS 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工信部等主管部门报告，并做出妥善安排。

9.10.3 效力的终止与保留

在本 CPS 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 CPS 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 CPS 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。订户或依赖方如有需要，也可以通过 SZCA 的联系方式向 SZCA 咨询了解 SZCA 终止的相关业务处理情况。

9.12 修订

9.12.1 修订程序

SZCA 将根据法律法规要求及业务实际需要，对 CPS 内容进行适当的必要的修改、调整。

具体修订程序详见本 CPS 1.5.4“CPS 批准程序”。修订版本的 CPS 将报工信部备案，且在 SZCA 的网站上公布，自公布之日起生效。

9.12.2 通知机制与期限

SZCA 有权修订本 CPS 中任何术语和条款，而且无须预先通知任何一方。

SZCA 在网站 https://www.szca.com 信息库中公布修订内容，及修订后的 CPS 完整版本，自修订后的 CPS 公布之日起该 CPS 生效。有关 CPS 修改内容的处理，以修改后的 CPS 条款为准进行。

SZCA 在认为有必要时，或应订户或依赖方请求，可以采取邮寄、电子邮件等的方式向上述主体在申请证书过程中提交的地址、邮箱，发送书面（包含电子 CPS）的 CPS。

若订户在修订后的 CPS 发布后 15 日内未提出证书吊销请求的，视为同意受该 CPS 约束。

9.12.3 业务规则必需修改的情形

如果出现下列情况，必须对 CPS 进行修订：

（1）密码技术出现重大发展，导致现有的 CPS 内容滞后性、不适应性；

（2）有关认证业务的相关标准发生改变；

（3）认证系统和有关管理规范发生重大升级或改变；

（4）法律法规和主管部门的要求；

（5）现有 CPS 出现重要缺陷；

（6）应用出现新的要求等。

对 CPS 的必要修订将在发布 15 日后生效，除非在 CPS 发布后的 15 日内，SZCA 以同样的方式发布撤消修订 CPS 的通知。

9.13 争议处理

在发生证书认证相关的纠纷，SZCA 运营安全管理小组专家组收集相关的证据，协调 SZCA 服务体系的各职能部门，决定是否批准通过争议解决报告，与订户等当事人进行沟通协商，促成和解或调解。

有关证书、CPS 及服务协议的适用、解释及执行的各种纠纷，进行诉讼的，应向 SZCA 登记注册所在地的有管辖权的法院提请诉讼。

9.14 管辖法律

本 CPS 依照《电子签名法》、《电子认证服务管理办法》以及其他中国现行有效的法律制定。

有关证书、证书策略及具体类型证书对应的 CPS 的任何争议，包括适用、解释、有效性等各种争议，无论订户或依赖方居住于何地或者其在何处使用证书，都应适用证书签发地，也即 SZCA 及其注册机构所在地（住所地）的法律，尤其是主要办事机构所在地或经常居所地的法律。

有关 SZCA 的证书、CP 及 CPS 的各种争议，都应统一适用中国的法律，除非当事人在合同中另行约定法律适用条款。

9.15 与适用法律的符合性

SZCA 的各项策略，均遵守并符合中华人民共和国的法律、和国家工信部等主管的要求。若本 CPS 中的任意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，直至该条款合法有效可执行为止。但本 CPS 某一条款或某些条款等部分条款的无效，不影响其它条款的法律效力。

9.16 一般条款

9.16.1 完整协议

本 CPS 将替代先前的与该主题相关的书面或口头说明、解释，并与订户协议、依赖方协议及其他补充协议构成 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暂停、终止电子认证服务，SZCA 的订户需按法律规定接受相应接管 CA 的证书服务的安排。

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 CPS 的任何条款或其应用，如果因为某种原因或在任何范围内部分条款被认定无效或不能执行，CPS 其余的部分仍然有效。电子认证法律关系相关参与方了解并同意，SZCA 的 CPS 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，及各种服务协议，均可独立于其它条款的个别条款，不因其他条款的解除、吊销、无效而无效，并可独立加以执行。

9.16.4 强制执行

未规定

9.16.5 不可抗力

本 CPS 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，如战争、政变、罢工、骚乱；

（4）互联网或其他基础设施无法使用等。

9.17 其它条款

SZCA 对本 CPS 拥有最终解释权。