深圳 CA 电子政务电子认证业务规则

深圳市电子商务安全证书管理有限公司

生效日期：2025 年 1 月 14 日

深圳 CA 电子政务电子认证业务规则

Shenzhen CA Certification Practice Statement for E-Government

2025 年 1 月 14 日

深圳市电子商务安全证书管理有限公司

https://www.szca.com

版权声明

深圳市电子商务安全证书管理有限公司（缩写为SZCA）完全拥有本文件的版权。本文件所涉及的“深圳CA”、“SZCA”及其图标等由深圳市电子商务安全证书管理有限公司独立持有，受到完全的版权保护。

其它任何个人和团体可准确、完整转载、粘贴或发布本文件，但上述的版权说明和主要内容应标于每个副本开始的显著位置。未经深圳市电子商务安全证书管理有限公司的书面同意，任何个人和团体不得以任何方式、任何途径（电子、机械、影印、录制等）进行部分的转载、粘贴或发布本CPS，更不得更改本文件的部分词汇进行转贴。

本CPS的最新版本请参见本公司网站https://www.szca.com/cps，除法律法规另有要求，不再针对特定对象另行通知。

深圳市电子商务安全证书管理有限公司对本CPS拥有最终解释权。

SZCA电子政务电子认证服务遵从中华人民共和国的法律，对于任何因违法行为而影响SZCA电子认证服务的个人、机构或者其它组织，SZCA将保留追究其法律责任的权利。

关于SZCA CPS中主要权利及义务的概要

1. 此概要仅是本CPS重要部分的简单描述，有关条款的完整论述以及其它重要条款和细节请看CPS正文全部内容。

2. 本CPS文件规定了SZCA电子政务电子认证服务的实施及使用，本CPS所指的电子认证包括证书发放、证书验证、证书管理等方面，从功能上讲，包括证书申请程序、证书申请的物理身份的验证、证书的签发、证书私钥的保护、证书的撤销和公布、证书的更新、证书状态的在线查询、证书的目录服务等。

3. 证书的申请者须知：

a) 申请者在申请证书之前，建议接受适当的数字认证相关方面的培训。

b) 从SZCA网站及其它渠道可以得到有关证书的CPS文件，证书申请者可以进行相关的学习。

4. SZCA提供不同类型的证书，申请者应自行或向SZCA咨询决定何种证书适合于自己的需要。

5. 证书申请者必须在接受证书后方可使用证书。申请者在接受证书的同时，就已表明其接受了本CPS规定的权利和义务，并承担相应的责任。

6. 证书依赖方必须自己决定是否信赖由SZCA签发的证书。在此之前，SZCA建议依赖方应检查SZCA的证书目录服务以确保证书是正确和即时有效的，签名是在证书有效期内使用创建的，而且有关信息并未改动。

7. 证书持有人同意，如果发生危及私钥安全状况时，及时通知SZCA及其授权证书注册机构。更多的信息请参看SZCA网站（https://www.szca.com）。

8. 意见与建议。任何人或者实体如果对以后CPS版本的编辑工作有任何意见或建议，请Email至：kfzz@szca.com.cn，或请邮寄至：深圳市福田区梅林街道孖岭社区凯丰路10号翠林大厦9层01、02、03、04-1、06、07、08号房（邮编：518000）。

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（以下简称“深圳 CA”或“SZCA”），成立于 2000 年 8 月 11 日，注册地广东省深圳市。2006 年 8 月 SZCA 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》，2007 年 10 月获得原信息产业部颁发的《电子认证服务许可证》，2010 年 11 月通过国家密码管理局的电子政务电子认证服务能力评估并取得电子政务电子认证服务资质。SZCA 将依照《中华人民共和国电子签名法》《中华人民共和国密码法》《商用密码管理条例》《电子认证服务管理办法》《电子政务电子认证服务管理办法》等法律、行政法规和电子政务电子认证服务技术规范、规则，在批准范围内提供电子政务电子认证服务。

SZCA 依据《电子政务电子认证服务业务规则规范》、GB/T26588《信息安全技术 公钥基础设施 证书策略与认证业务声明框架》等制定《电子政务电子认证业务规则》，并将其命名为《深圳 CA 电子政务电子认证业务规则》（简称“电子政务 CPS”或“本 CPS”）。电子政务 CPS 是 SZCA 提供电子政务电子认证服务过程中所应遵循的业务规则，是关于电子政务电子签名证书生命周期管理全过程（含证书管理<包含发布和存档>、吊销、挂起、变更、更新证书或密钥更新）的业务实践的完整声明和详细描述，包括业务运营操作、技术与法律责任等方面内容，本 CPS 阐述了 SZCA 签发、管理证书以及证书运营维护服务的各种活动、基础设施技术要求，及提供实际工作运营中所遵守的规范。

本 CPS 适用于电子政务电子认证服务活动中的 SZCA 及其授权注册机构、订户、依赖方与其他电子政务电子认证参与方。所有相关参与人都必须完整地理解和执行本 CPS 规定的条款，并依此行使权利和履行义务。

SZCA 的根证书体系见附录一。

1.2 电子政务电子认证业务范围

电子政务认证机构面向电子政务活动中的政务部门和企事业单位、社会团体、社会公众等电子政务用户提供证书申请、证书签发、证书更

新和证书撤销等证书全生命周期管理服务。

1.3 电子政务电子认证活动参与者

1.3.1 电子政务认证机构

电子政务电子认证机构，即电子政务电子认证服务机构，简称 CA、电子政务 CA，是面向电子政务用户提供的证书申请、证书签发、证书更新和证书撤销等证书全生命周期管理服务的实体。同时电子政务 CA 区别于注册机构，在于仅电子政务 CA 有权签发证书、发布证书撤销列表（CRL）、发布电子政务 CPS、CP。

SZCA 是依法设立的电子政务电子认证服务机构。

1.3.2 注册机构

注册机构，是为最终证书申请者建立注册过程的实体，负责面向最终用户受理数字证书的新办、更新、变更、挂起、撤销、介质补办、密钥更新与密钥恢复等业务申请，对证书申请者进行身份标识和鉴别，发起或传递证书请求，代表电子认证服务机构（含电子政务电子认证服务机构）处理、批准证书申请，并承担用户通知、证书制作下载交付等具体证书办理工作职责。

SZCA 的注册机构（以下简称“RA”）是经 SZCA 授权运营的负责面向最终用户受理证书业务申请的实体，包括内部的业务组织、下属机构（含分公司、营业部、受理点），及独立于 CA 的外包第三方机构。SZCA 注册机构的名单，由 SZCA 对外予以公布。SZCA 注册机构的授权业务范围取决于 SZCA 指定，或合同约定情况。外部注册机构需按照与 SZCA 签订的书面协议在约定的授权范围开展业务活动，对外应以 SZCA 注册机构或代理机构名义开展证书受理业务。本 CPS、CP 及其他 SZCA 制定的有关注册机构运营、服务方面的规范文件，自动构成 SZCA 与注册机构合作协议的附件。

注册机构应履行本 CPS、CP 中注册机构相关章节规定的注册机构的职责和义务，严格按照 SZCA 制定的 CPS、CP 及业务规范开展证书注册业务，不得再对外转授权、转分包注册机构。

1.3.3 依赖方

依赖方，又叫证书依赖方、电子签名依赖方，是指依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是也可以不是一个证书持有者。依赖方既可以是订户、也可以不是订户。

具体而言，依赖方，可能是依赖 SZCA 签发的证书进行网上业务往来的订户，也可能是依据本 CPS 合理信任 SZCA 签发的证书真实性的任何实体。

通常情况下，依赖方应合理地信任证书以及相关的数字签名。如果信任数字签名时需要获得额外保证或履行适当的注意义务，依赖方应在得到这些保证或完成这些检查确认后方可信任该数字签名。

1.3.4 其他参与者

（1）订户

订户，即证书持有人、最终用户，是指从 SZCA 接受证书实体，也是持有证书、使用证书且需为合法使用其证书行为承担法律责任的实体。在电子签名应用中，订户即为电子签名人。

SZCA 建议订户在申请证书之前阅读熟悉 SZCA 的 CPS、CP 相关文件，了解数字证书及其相关产品的用途功能、使用条件、注意事项、法律风险及法律后果。订户可以从 SZCA 网站、业务受理点或联系 SZCA 获取 CPS、CP、业务办理指南、服务手册等文件资料。

（2）其他参与者

为以上未提及电子政务电子认证服务活动中涉及的其它实体，例如 SZCA 证书制作机构、证书信息库服务提供者、时间戳服务提供者以及其他提供电子政务电子认证相关服务的实体。

1.3.5 各方主要责任

(1)CA 的责任

SZCA 应按照法律、行政法规、部门规章及 CPS、CP 相关要求开展数字证书申请、受理、审核、签发（含发布）、更新、变更、挂起、撤销相关证书声明周期管理服务。

签发、更新、撤销证书后，SZCA 应发布证书或证书撤销信息，提供证书信息查询、证书状态查询服务。

SZCA 应按照要求完整记录、保存与电子签名认证相关的信息。

SZCA 应当遵守国家有关密码管理要求，保障电子政务电子认证服务使用密码安全。

SZCA 应保障电子认证服务系统及其设备设施的安全稳定运行。

SZCA 应对其授权的证书注册机构的证书注册业务进行管理、监督和审计。

发生影响证书使用的技术革新、安全事件，SZCA 应及时提醒通知证书订户及时更新证书及其软硬件以保证证书的可靠性。

(2)注册机构 RA 的责任

RA 应在授权范围内以 CA 的注册机构或代理机构名义依法开展注册业务。并积极配合 RA 的业务管理、检查、监督工作，配合参加业务培训、主管单位的注册机构业务备案及业务合规评估、检查工作。

RA 应根据本 CPS 第 2 章 “2 身份标识与鉴别”、第 3 章“3.数字证书服务操作规范”等相关章节规定、CP、与 SZCA 书面协议等的相关规定，及其它 SZCA 公布或提供的证书业务流程、要求和标准，依法受理证书申请者的证书申请。

受理电子签名认证证书申请时，注册机构应当对申请人的身份进行查验，对有关申请材料进行审查，并向申请人告知电子签名认证证书和电子签名的使用条件、电子签名所产生的法律责任、保存和使用电子签名认证证书持有人信息的权限和责任、电子政务电子认证服务机构和电子签名认证证书持有人的责任范围等事项。受理证书申请后，将确保订户与 CA 签订书面服务协议，并将证书或证书密码、口令等以安全方式交付给用户。因为 RA 对申请者的风险提示与业务告知不充分、资料审核不严、证书发放或通知不规范等导致的证书办理、使用的纠纷产生的所有损失，由 RA 承担。

注册机构完整记录和保存与电子签名认证证书注册业务相关的信息，包括证书申请人申请、更新、变更、撤销证书等业务时证书申请、审核、受理、通知、签发、接受等全过程业务环节的信息，如证书申请材料、鉴证材料、交付证明资料、证书发放通知等，并按 SZCA 要求向 SZCA 提供 SZCA 指定的证书服务数据资料，且应保证证书业务过程具有可追溯性，如注册机构自行保存注册业务信息的，信息保存期限至少为电子签名认证证书失效后 5 年。

注册机构应对其在证书注册工作中知悉的国家秘密、商业秘密和个人隐私承担保密义务，采取相应的技术措施和其他必要措施保护有关信息和数据安全。

RA 应确保业务运营系统处在安全的物理环境与网络环境中，并采取必要的技术措施保障 RA 与 CA 之间的数据传输安全，保证依法使用 SZCA 颁发的操作员证书或管理员证书，不得转让或提供他人使用，并保证依法使用 SZCA 的证书相关技术接口及其开发工具、接口文档，未经 SZCA 授权不得提供、转接、转授权给第三方使用。

(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生成、持有、保管及安全保存的相关程序：

(a) 证书申请者须保证在证书申请表上填列的声明和信息，或其他提交的资料、陈述的信息是完整、准确、真实和可供发证机构查实的；并承担一切因提供虚假信息所造成的法律后果。并同意配合 SZCA 与其授权注册机构进行相关验证、审核工作，同意授权 SZCA 与其授权注册机构采取有效途径向第三方机构查询核验用户提交、陈述的信息的真实性有效性。

(b) 证书申请者在申请证书前，需要了解本 CPS、CP 及订户服务协议相关规定，了解证书的用途、使用条件、使用目的、法律风险及法律后果。

(c) 证书申请者自行或委托第三方生成证书密钥对的，证书申请者须了解并遵循本 CPS 所述条款，充分了解私钥安全生成保存的重要性，确保证书私钥的安全性并承担所有因订户的私钥安全问题产生的法律责任。

SZCA 在接到证书申请者的证书申请时即认为该申请者已经了解本 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

证书申请者完成证书业务办理，接受证书后，即成为证书订户。

订户必须确保将持有的证书用于申请时预定的目的，在证书用途范围内按照约定的业务目的依法使用证书。

订户有责任保证私钥的安全。订户应妥善保存及安全保护证书私钥及相关密码、口令、密钥令牌等，采取合理措施防止私钥的遗失、泄露、被篡改、损害或被未经授权使用。SZCA 并不强制要求证书申请者选用 SZCA 提供的密钥生成保管安全措施；订户可以选择任何自己认为可行的保密措施，但需承担因此产生的法律责任。

对于任何实际发生或可疑的证书密钥遗失、泄密或其他对私钥的安全威胁，订户都应立即通报给 CA 或 RA，采取申请证书挂起撤销等处理措施。由于通知延误、或使用不安全证书所造成一切损失由证书订户自行承担。

签名时，电子签名人应检查证书确保证书是订户接受的有效证书（证书没有过期、挂起或撤销）。订户接受证书后，除非有相反证据证明，使用证书中所含公钥相对应的私钥所进行的每一次签名，都视为订户的签名。

证书中的所含的订户身份信息（如个人姓名、身份证号，或机构名称、统一社会信用代码，户籍地或住所地）或其他订户信息（如角色、岗位、职位、附属关系）等发生任何改变，订户应通报给 CA 或 RA。

(5)依赖方的责任

依赖方在信赖任何 SZCA 签发的证书的时候，必须保证遵守以下条款：

(a) 依赖方了解本 CPS 的条款以及和证书相关的证书策略，了解证书的用途功能、使用目的；

(b) 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 显示该证书已撤销作废，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本 CPS 的有关条例包括有关免责、拒绝和限制权利的条款。

(6)其他参与者的责任

SZCA 的证书制作机构，应确保制作的证书格式符合《电子认证服务管理办法》《电子政务电子认证服务管理办法》及国家标准等技术规范的要求，保证证书内容的准确性可用性。

证书信息库服务机构，应确保及时准确在 LDAP 目录服务器上发布证书订户的证书公开信息及证书 CRL。

SZCA 的时间戳服务机构，应确保提供的时间戳时间的准确性，保证时间数据来源于国家权威时间源。

1.4 电子政务电子认证策略管理

1.4.1 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”由公司运营人员、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。任何有关 CPS 的问题、建议、疑问等，都可以与“SZCA CPS 策略发展小组”联系反馈。SZCA 欢迎并将慎重对待来自社会各群体对于本 CPS 的意见和建议。

1.4.2 联系方式

如有需要，请联络：

收件人：深圳市电子商务安全证书管理有限公司

联系部门：SZCA CPS 策略发展小组

电话：0755-26588388

电子邮件：kfzz@szca.com.cn

邮寄地址：深圳市福田区梅林街道孖岭社区凯丰路 10 号翠林大厦 9 层 01、02、03、04-1、06、07、08 号房【邮政编码：518000】

官网地址：https://www.szca.com

CPS 发布地址：https://www.szca.com/cps

1.4.3 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 修订稿），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 安全策略管理委员会”审阅。经该组织审议、审核通过后，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 安全策略管理委员会”审批意见及 CPS 电子版存档。

自发布之日起，各种形式对外提供的 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 公布后向主管部门备案。

1.5 定义和缩写

表1.1-定义与缩写

缩写/名词	定义
SZCA	Shenzhen Certificate Authority,深圳市电子商务安全证书管理有限公司的英文名称缩写，也称深圳CA。
电子认证服务机构	英文名称Certificate Authority、Certification Authority，缩略语CA，对数字证书进行全生命周期管理的实体，也称证书认证机构。
电子政务电子认证服务机构	英文名称E-government CA，也称电子政务CA，对电子政务数字证书进行生命周期管理的实体。
注册机构	英文名称Registration Authority，缩略语RA，是指面向最终用户受理证书的申请、更新、恢复和注销等业务的实体，可以是CA的内部职能部门、分支机构、分公司、受理点、营业部等，也可以是授权的外部的第三方机构。 具有下列一项或多项功能的实体：标识和鉴别证书申请者，同意或拒绝证书申请，处理证书申请。但RA并不签发证书。
证书注册受理点	英文名称Local Registration Authority，缩略语LRA，是指本地设立的受理数字证书业务的服务网点。
注册机构协议	CA机构与证书注册机构缔结的关于注册机构服务内容与要求，业务流程与规则、责任和义务的合同文件。
电子认证业务规则	又称证书业务声明，英文名称Certification Practice Statement，缩略语CPS，是CA机构公开发布的在证书颁发中所遵循的业务实践的声明，是关于证书生命周期管理业务实践的详细描述，并且包括证书签发与管理、密钥管理业务、技术、法律等方面细节内容。 电子政务电子认证业务规则，指电子政务电子认证服务机构发布的关于电子政务电子认证证书的生命周期管理过程、PKI设备设施运营管理、法律责任等业务实践的详

	细描述。
证书策略	英文名称Certificate Policy,缩略语CP，是用以指明证书对具有相同安全需求的一个特定团体和/或应用类型适应性的一套规则集。
证书申请者	证书申请者（Certificate Applicant）是指请求CA颁发证书的个人、企业或其他组织机构。
订户	被CA机构颁发证书并接受、持有、使用证书的实体，包括个人、企业、政府事业单位等。 在证书申请时，被称为证书申请者。在接受证书后被称为证书持有人、订户。在签名时被称为电子签名人。
依赖方	依赖方（Relying Party）指依赖于数字证书或通过数字证书所验证的数字签名真实性而从事相关业务活动的实体，也是使用公钥证书验证数字签名有效性的主体。也称证书依赖方、电子签名依赖方、证书使用者。
OCSP	OCSP（Online Certificate Status Protocol），即在线证书状态协议， 用于支持实时查询数字证书状态。
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撤销列表（CRL）。
PKI	PKI（Public Key Infrastructure），公开密钥基础设施，支持公钥管理体制的基础设施，提供鉴别、加密、完整性和不可否认性服务。
CRL	英文名称Certificate Revocation List（缩略语CRL），即数字证书撤销列表、证书吊销列表、证书黑名单。CRL中记录所有在原定失效日期到达之前被撤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。内容通常还包含 CA机构的名称、发行日期、下次撤销列表的预定发行日期、变更或撤销的数字证书序号，并说明变更或撤销的时间。
数字证书	英文名称digital certificate，也称证书、公钥证书、电子认证证书、电子签名认证证书，由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。
电子签名	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。
证书口令	证书口令，又称PIN码、证书密码，指证书私有密钥的保护口令。
证书序列号	英文名称 certificate serial number，指CA颁发证书为每一张证书分配的一个唯

	一的用于标识证书的整数值。
甄别名	英文名称Distinguished Name，缩略语DN，包含用户的身份信息（如名称、姓名）和其他属性信息。
私钥	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(签名私钥)，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（加密私钥）。 电子签名制作数据即为签名私钥。
公钥	公钥是经由数字运算产生的密钥，可用于验证电子签名，确认电子签名人的身份及电子签名的真实性，或解密经加密的数据。 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。 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（签名）私钥，则电子签名验证数据就是（签名）公钥。
签名密钥对	证书申请者申请证书时由用户端产生，包含一对私有密钥和公开密钥，主要用于用户的签名和验证。
加密密钥对	证书申请者申请证书时由 KMC 产生，包含一对私有密钥和公开密钥，主要用于用户信息的加解密。
PKCS	PKCS （Public Key Cryptography Standard），公开密钥密码算法标准。
SZCA数字证书签发系统	为证书申请者签发、发布、管理数字证书的SZCA软件系统。
密钥管理中心	简称 KMC，负责密钥的产生、存储、归档等工作。
SZCA CPS策略发展小组	由SZCA任命的负责CPS、CP的修订、日常维护管理与咨询的组织。
SZCA安全策略管理委员会	由SZCA任命的负责SZCA安全策略核准及执行的组织。
SZCA超级管理员	SZCA指定的负责实施 CA政策、增加新 CA管理员、验证审计记录、执行电子认证业务规则与证书策略要求的角色。
SZCA系统管理员	SZCA指定的负责安装、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的角色。
SZCA录入员	SZCA指定的负责录入证书申请者提交的信息的角色。

SZCA审核员	SZCA指定的负责审核证书申请信息的角色。
SZCA审计员	SZCA指定的负责CA系统的证书统计、系统审计等工作的橘色。
SZCA证书制作员	SZCA指定的负责为证书申请者制作证书的角色。

1.6 策略发布与管理

1.6.1 策略的发布

CPS、CP 通过 SZCA 官网发布，订户协议（即 SZCA 的电子认证服务协议）、依赖方服务协议（如有）等服务协议、规范文件、公告通知等通过 SZCA 官网 https://www.szca.com 、或服务平台发布。

1.6.2 策略发布的时间与频率

SZCA 将根据法律法规政策、技术发展、及业务实际，定期检视、适时修订 CPS 内容，并及时发布 CPS 的最新版本。一旦对规则的修改、补充等获得批准，如无特殊情况发生，SZCA 将在 5 个工作日内在官网 https://www.szca.com 上发布。

1.6.3 策略访问控制

SZCA 设置了信息访问安全控制和安全审计措施，保证只有经过授权的 SZCA 工作人员才能编写和修改 SZCA 官网公告和信息库发布的信息。除非订户、依赖方提出异议，SZCA 将发布相关认证证书信息到信息库中。SZCA 一般不限制社会公众访问 CPS、CP、订户协议、依赖方服务协议（如有）等服务协议、规范文件、公告通知等。公钥证书、CRL、LDAP 等信息库发布的证书、证书状态等信息如涉及需要保密的个人信息或商业秘密信息，SZCA 在认为必要时，可采用安全控制、清除程序或其他技术措施，仅对订户指定的对象提供证书信息或提供证书状态查询渠道，或对涉敏信息项作出存在但公众不可查看、不可使用的标识。

2 身份标识与鉴别

2.1 数字证书命名与格式

2.1.1 证书命名

SZCA 颁发的证书，含有颁发机构和证书订户的主体甄别名，订户的甄别名（Distinguished Name）用以标识证书持有人或证书主体的名称及其他属性信息。SZCA 颁发证书前对证书申请者的身份和其它属性进行鉴别，并以不同的标识（含订户甄别名、主体可选替换名称或其他扩展项）记录其信息。订户的证书甄别名，是证书中证书持有者的唯一识别名。SZCA 分配给证书持有者的证书的甄别名符合 X.509 标准、GM/T0015，不使用匿名或假名。

表3.1-CA颁发机构甄别名

属性	值
通用名（CN）	SZCA
机构（OU）	SZCA
机构部门（O）	ShenZhen Certificate Authority
城市（L）	Shenzhen
省份（ST）	Guangdong
国家（C）	CN

表3.2-最终订户甄别名命名规则

属性	值
通用名（CN）	● 机构名称（适用于机构证书）； ● 个人姓名（适用于个人证书、机构个人证书）； ● 设备名称或其他设备唯一标识信息（适用于设备证书）； ● 电子邮箱地址（适用于电子邮箱证书）； ● 或其他自定义的包含上述信息及附加标识（含应用平台名称、项目名称等）在内的组合名称
机构（O）	● 订户（如为机构证书、个人证书、机构个人证书）或证书主体（如设备证书、电子邮箱证书）所在单位、所属机构的名称【如

	存在所属机构、可获取查询到该机构信息】；或 ● 证书应用平台标识信息（适用于个人证书）或订户住所地信息【如不存在所属机构，或所属机构信息无法获取核实的】； ● 其他自定义的与订户、证书应用关联的标识信息
机构部门（OU）	可以包含以下一个或多个内容： ● 订户、证书主体在所属机构的内部职能部门、下属部门或分支机构名称； ● 或引用依赖方协议的一个声明，该依赖方协议明确的使用证书的条款； ● 通告描述证书类型、证书应用标识、证书鉴别方式等内容的相关文字字符
城市（L）	订户或证书主体所在城市，或不填
省份（ST）	订户或证书主体所在省份，或不填
国家（C）	订户或证书主体所在国家，其中CN表示中国
电子邮件（E）	订户的电子邮件地址，或不填

2.1.2 证书版本

SZCA 签发的证书符合 X.509 V3 版证书格式。

2.1.3 证书扩展项

1、证书标准扩展项

- 颁发机构密钥标识符(Issuer Unique Identifier、authorityKeyIdentifier)：此域用在当同一个 X.500 名字用于多个认证机构或同一 CA 机构的多张公钥证书时，用来标识区分签发者的密钥证书。CA 以“自签”证书形式发放公钥时，此项可省略，此时主体密钥标识符和认证机构密钥标识符完全相同。
- 主体密钥标识符（Subject Unique Identifier）：此域用在当同一个 X.500 名字用于多个证书持有者或同一证书持有者的多张公钥证书时，用来标识区分证书持有者的密钥证书。
- 密钥用法（key Usage）：指定各种密钥的用法：数字签名、不可抵赖/不可否认、密钥加密、数据加密、密钥协议、验证证书的 CA 签名、验证 CRL 的 CA 签名、只加密、只解密、只签名。

- CRL 发布点：由 SZCA 定义的 CRL 发布点，标识如何获得 CRL 信息。
- 证书策略（certificate Policies）：列出颁发证书的 CA 所认可的证书策略，该策略适用于证书及关于证书策略的任选的限定符信息，至少包含一个 OID 和一个可选的限定条件。
- 主体替换名称（subjectAltName）：包含一个或多个主体的可选替换名，并由 CA 与证书主体的公钥绑定，该项可包含主体的附加身份，电子邮件地址、DNS 名称、IP 地址和 URI
- 基本限制（basicConstraints）：标识证书主体是否是一个 CA，通过该 CA 可能存在的认证路径有多长。
- 名称限制（name Constraints）：只用于 CA 证书，指示一个名称空间，该控件设置了认证路径中后续证书的所有主体名称。
- 策略限制（policy Constraints）：用于向 CA 颁发的证书中，用来禁止策略映射或要求路径中的每个证书包含一个认可的策略标识符。
- 策略映射（policymappings）：仅用于 CA 证书，列出一个或多个 OID 对，每对包括一个 issuerDomainPolicy 和一个 subjectDomainPolicy，以告知用户 CA 的策略同用户接收到的发行方 CA 策略是等效的。
- 扩展的密钥用法(extKeyUsage)：指明已验证的公开密钥可用于一种或多种用途，它们可作为对密钥用法扩展项中指明的基本用途的补充或替代，如鉴别、邮箱保护。
- 其他 RFC5280 规定的证书扩展项。

2、自定义扩展项

自定义扩展项，也称专用扩展项，是 SZCA 针对特定的证书应用自定义的适用特定场景、项目的证书扩展项，主要包括但不限于以下扩展项：

（a） 企业标识：指定企业的唯一标识符。

（b） 市电子政务实体唯一标识：代表证书持有者身份的唯一编码，可与业务系统的用户账号绑定关联。

（c） 组织机构代码：机构的组织机构代码。

（d） 注册号：指定机构的注册号。

（e） 统一社会信用代码：指定机构的统一社会信用代码。

（f） 登记机关：指定机构、企业的登记机关。

（g） 法人(负责人)：指定机构、企业的法定代表人或负责人名称。

（h） 身份证号：指定机构、企业的法定代表人或负责人，或个人的身份证号。

（i） 岗位名称：指定机构、企业内工作岗位的名称。

（j） 机构签名证书序列号：指定机构、企业的证书中签名证书序列号。

（k） 业务/场景属性：指定证书所适用的业务属性。

（l） 项目类型：指明证书所应用的项目类型、或行业应用类型

（m） 扩展代码：指定机构/企业业务证书颁发的数量。

（n） 扩展标识：指定项目证书应用或证书主体标识所需信息。

（o） OA 号：指明证书主体或证书应用相关的标识信息，或其他未经验证的订户信息。

（p） 岗位责任人：指定机构/企业业务证书中所在岗位的责任人。

（q） 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。

（r)深圳 CA 扩展标识：深圳 CA 的其他标识性信息。

（s)卫生系统唯一标识：用户在卫生系统对应的业务唯一标识。

2.2 身份标示与鉴别

2.2.1 证明拥有私钥的方法

证明证书申请者拥有私钥，CA 通过 PKCS#10 等数字签名技术验证签名密钥属于证书申请者，具体方式为使用证书申请者公钥验证其私钥签名的有效性和证书申请数据的完整性。

2.2.2 组织机构身份鉴别

对组织机构的身份鉴别，包含组织机构的身份、经办人/授权代表/授权代理人的身份、组织机构中个人的身份（如涉及机构个人证书申请），及授权代表授权有效性的核验，具体鉴别验证内容、方式及其流程如下：

（1）核查提交的用户申请资料、信息是否完整、齐全、填写准确；

（2）核对各项申请材料、各申请环节中经办人/授权代表/授权代理人身份信息、机构身份信息、法定代表人或负责人身份信息、机构个人身份信息是否一致、相符、相匹配；

（3）组织机构的合法真实存在、机构信息真实有效，可通过查询

国家企业信用信息公示系统、全国组织机构统一社会信用代码查询平台（即全国组织机构统一社会信用代码数据服务中心）、信用中国等国家工商数据库、企业征信数据库、信用平台或其他合法可靠的第三方企业数据库，或咨询登记注册管理部门，或通过机构官网公开或其在政府、主管机关处注册备案的电话、电子邮箱、地址等联系机构与其确认、实地调查等方式来验证；同时还可辅助参考办证时组织机构近6个月的水、电、电信服务缴费凭证、纳税证明、银行开户或其他银行业务办理证明等机构对公业务办理材料判别机构是否有效存续运营；

（4）对于个人身份的核验，包括机构经办人/授权代表/授权代理人、各机构个人身份鉴别，可通过公安部“互联网+可信身份认证平台”（CTID平台）、全国公民身份信息系统（即全国公民身份证号码查询服务中心）、出入境证件身份认证平台等国家身份认证平台、驾驶证查询系统等国家身份信息权威数据源查询，或采取人脸识别等生物特征识别技术，或进行电信验证、金融银行卡认证等手段，验证相应个人身份的真实性；机构个人身份的验证，还可由机构提供机构个人用户名单、录入或提供机构个人信息，SZCA 通过适当的辅助手段验证其身份真实性。

（5）对于组织机构经办人/授权代表/授权代理人的授权的确认，可依靠机构盖章的业务办理授权文件，全国银行开户行联行号查询网查询，组织机构金融账户小额打款回填验证码，企业法定代表人/负责人人脸识别、法定代表人/负责人手机验证码短信回填等方式辅助验证，通过机构官网公开的或其在政府、主管机关处注册备案的电话、电子邮箱、地址等联系方式与机构确认，或其他 SZCA 认为合理的方式，来确认该机构知晓并授权证书申请，代表组织机构提交证书申请的人是经过授权的。

2.2.3 个人身份鉴别

SZCA 使用以下两种或以上手段进行认证，包括但不限于身份证读卡机具等软硬件设备方式鉴别证件真伪，公安部“互联网+可信身份认证平台”（CTID 平台）、全国公民身份信息系统（即全国公民身份证号码查询服务中心）、出入境证件身份认证平台等国家身份认证平台、驾驶证查询系统等国家身份信息权威数据源查询，采取金融银行卡认证、手机号电信验证，面对面审核及人脸识别等生物特征识别技术，电话确认、信函确认、上门实地调查、远程视频验证等手段措施个人是真实存在的

且身份信息真实。

2.2.4 政府部门个人身份鉴别

在把证书签发给政府部门中的个人时，SZCA 还应确认以下内容：

1）通过与政府部门电话、书面核实个人任职部门、岗位等可靠的方式，确保证书持有者所在的组织、部门与证书中所列的组织、部门一致，证书中通用名就是证书持有者的真实姓名；

2）确认证书持有者属于该组织机构，证书持有者确实被招录或聘用。

同时，如通过第三方合作机构发起的证书申请，还可委托第三方合作机构进行辅助验证审核，第三方合作机构应对审核的内容信息的真实性有效性承担责任。

如 SZCA 无法通过前述途径获得证书认证、制作、发放所需信息，或无法有效验证申请者，可委托第三方进行调查，或要求证书申请者提供额外的信息和证明材料，配合进行其他补充验证，申请者必须保证所提交的补充材料的真实性，SZCA 和其授权的证书注册机构将对申请者的材料依法进行审查。

境外国家、地区的机构、个人的身份鉴别，SZCA 可依据我国关于境外法律文件在我国采纳作为证据所规定的公证认证相关规则执行；同时 SZCA 有权决定采用其他认为可靠的方式认证境外机构与人士。

SZCA 保留根据国家法律法规、政策规定更新身份鉴别规范的权利，更新后的身份鉴别规范将发布在 SZCA 的网站。

SZCA 授权的注册机构，应按照 SZCA 个人身份鉴别规范对用户的证书申请进行审核，并根据鉴别结果进行批准或驳回申请的操作。

2.3 密钥更新请求的标识与鉴别

2.3.1 常规密钥更新的标识与鉴别

对于一般正常情况下的密钥更新申请，根据密钥更新原因、更新时间、业务类型的不同，密钥更新的标识与鉴别流程区分如下：

（1）证书有效期内的证书密钥更新，包括证书密钥更新、证书补办：

(a) 证书密钥更新，用户可使用原证书私钥对包含新公钥的申请信息签

名后提交申请，无需提交身份证明资料，SZCA 用原证书（有效期内的证书）上的证书持有者公钥对申请的签名进行验证、验证原证书口令进行鉴别；用户也可选择按照证书申请流程提出申请，鉴别流程参见本 CPS“2.2 身份标示与鉴别”有关规定。

(b) 证书补办，证书补办业务的操作流程，按照证书申请的身份鉴别和受理流程执行，具体按照本 CPS “2. 身份标识与鉴别”及第 3.1-3.4 章规定进行。证书补办是指在证书有效期内，证书持有者出现证书载体丢失或证书载体损坏时进行证书补发的操作。补发操作成功时，旧证书将被撤销，新证书有效期从新证书签发之日起到旧证书有效截止日期/失效日止。

（2）证书有效期满后的证书密钥更新

即证书更新续期，用户应提交证书新申请相关申请材料，鉴别流程参见本 CPS“2.2 身份标示与鉴别”。

2.3.2 撤销后密钥更新的标识与鉴别

证书撤销后不能进行密钥更新。

证书撤销后的密钥更新，须订户申请新证书，鉴别流程见本 CPS“2.2 身份标示与鉴别”。

2.4 撤销请求的标识与鉴别

当证书持有者提出证书撤销申请，且满足本 CPS“3.8 证书撤销”所述撤销情形时，SZCA 注册机构应当审核撤销申请者的书面申请材料（含证书 DN 信息），鉴别申请人身份，审核通过后向 SZCA 提起撤销申请，由 SZCA 执行撤销操作。撤销的识别与鉴别流程见本 CPS “3.8.4 证书撤销的鉴别”。

SZCA、注册机构、司法机关，在订户未履行 SZCA CPS 或服务协议所规定的义务等订户原因，因密钥失密等客观原因造成证书应予撤销的，可发起证书撤销，此时不需要对订户身份进行标识和鉴别。

证书撤销后将 SZCA 或其授权机构将通知证书订户。

3 数字证书服务操作规范

3.1 证书申请

3.1.1 证书申请流程

1、机构证书的申请流程

组织机构在申请证书时，应授权指定合法的证书申请经办人或代理人，提交证书申请材料，并代表机构签署相关服务协议等文件（含《数字证书申请表》、《电子认证服务协议》）。

证书申请材料通常包括如下资料，具体以项目中 SZCA 对外通知公告的资料要求为准：

1)机构登记、成立的有效身份证明文件、信息，机构法定代表人或负责人的身份证明文件、信息；

2)经办人或代理人的有效身份证明文件、信息；

3)授权委托书或《数字证书申请表》（需盖章）；

4)《电子认证服务协议》《个人信息授权书》（需盖章或经办人签署）。

（1）机构有效证件

组织机构合法有效的身份证明文件，包括但不限于如下：

（a)工商营业执照、税务登记证、组织机构代码证、统一社会信用代码证（适用于公司企业、个体工商户、合伙企业、个人独资企业、农民专业合作社等商事组织）；

（b)法人登记证，如事业单位法人证书、社会团体法人登记证、基金会法人登记证等（适用于非商事法人主体）；

（c)民办非企业单位登记证书、外国（地区）企业常驻代表机构登记证、政府部门颁发的许可证（含律师事务所执业许可证、金融机构法人许可证、金融机构营业许可证、医疗机构执业许可证等）；上级单位（如政府）的批文或特许文件（适用于政府机关）；

（d)其他民政、工商、机构编制管理部门等有关政府机构颁发、出具的机构注册设立的有效证明文件。

（2）证书办理渠道与要求

机构证书的办理方式包括：

1) 线下方式：

包含面对面、邮寄等办理方式。组织机构授权的经办人/授权代表/

授权代理人按照要求填写提交证书申请材料，其中机构的身份证件复印件、法定代表人或负责人的身份证复印件、经办人或代理人的身份证复印件需加盖公章，《数字证书申请表》或《授权委托书》，及《电子认证服务协议》《个人信息授权书》等需填写完整并加盖公章、签字，现场办理的经办人需携带本人有效身份证件原件现场提交校验。

2) 线上方式：

组织机构经办人/授权代表/授权代理人可通过 SZCA 的自有平台、或授权合作的第三方机构线上平台提交证书办理申请，应提交申请人身份证件电子影印件，如含营业执照在内的有效机构登记证件、法定代表人或负责人身份证电子影印件（或机构名称、统一社会信用代码、机构法定代表人/负责人姓名及其身份证号信息），经办人/授权代表/授权代理人身份证电子影印件（或个人姓名、身份证件号码），上传提交盖章的《授权委托书》或《数字证书申请表》，及《电子认证服务协议》《个人信息授权书》，或通过在线数据电文方式签署《电子认证服务协议》《个人信息授权书》。并应在 SZCA 认为必要时，配合 SZCA 进行机构银行账户小额打款验证码回填、人脸识别等验证工作。

同时申请机构个人证书的，机构及其经办人/授权代表/授权代理人应确保得到各机构个人合法有效的授权及保证提交的机构个人信息真实有效准确，组织机构的经办人/授权代表/授权代理人还应提交各机构个人有效身份证件复印件（须盖章），或机构个人办证清单、承诺书等资料（须盖章，含制作证书所必需的信息）。

2、个人证书的申请流程

（1）个人有效证件

个人身份鉴别可以使用以下有效的身份证件：

- 身份证，在特殊情况下户口簿、驾照、护照、有效期内的临时身份证可作为辅助证明证件（适用于大陆居民）；
- 军官证、警官证、文职干部证、文职人员证、军队学员证、军士证、警士证、士官证、义务兵证、士兵证、残疾军人证等（适用于军警人员）；
- 港澳居民来往内地通行证、台湾居民来往大陆通行证（即“回乡证”，适用于港澳台同胞）；
- 外国人永久居留证件（含外国人永久居留身份证、处于有效期内

旧版现行外国人永久居留证）、护照(适用于外国人)；

- 其他政府颁发的有效身份证件。

（2）证书办理渠道与要求

SZCA 的个人证书的办理方式包括：

1) 线下方式

包括面对面和邮寄方式。

现场办理的，个人应持上述个人有效身份证件原件，亲自到 SZCA 授权的注册机构受理网点，当场提交个人身份证影印件、填写签署《数字证书申请表》《电子认证服务协议》《个人信息授权书》等申请材料。

邮寄办理的，个人应扫描身份证复印件、并下载填写签署《数字证书申请表》《电子认证服务协议》《个人信息授权书》等申请材料，邮寄给 SZCA 或其授权注册机构。并应在 SZCA 认为必要时，配合 SZCA 进行电话、短信回填、电信手机号三要素（姓名、身份证证号、手机号）、银行卡四要素（姓名、身份证证号、银行卡号、银行预留手机号）、人脸识别验证等补充提交信息或补充验证工作。

2) 线上方式

个人可通过 SZCA 的自有平台、授权或合作的第三方机构线上平台提交证书办理申请，应提交本人身份证件电子影印件（或姓名、身份证件号码身份信息），提交手写签字的《电子认证服务协议》《个人信息授权书》复印件或以数据电文方式在线签署《电子认证服务协议》《个人信息授权书》。并应在需要时配合 SZCA 进行人脸识别、手机短信验证码回填等验证工作。

需由证书申请者承担证书费用的，证书申请人应完成证书服务费用缴纳。

SZCA 可通过发布证书办理指南、证书风险提示、证书服务手册等方式向用户告知证书申请流程，证书申请资料要求，证书申请办理，方式证书用途功能、使用条件与法律后果等内容。

3.1.2 证书申请实体

任何具有完全民事行为能力的自然人、依法注册成立的企事业单位、社会团体等各类组织机构，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；机构证书（含机构个人证书）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/使用人或其被授权人（如设备所有人/使用人为机构）提出申请。经办人/授权代表/授权代理人代表机构进行批量证书申请的，还应确保获得机构的授权。

RA 向 SZCA 提交证书申请的（RA 操作员证书、管理员证书除外），应确保证书申请来自于证书主体，且已就证书申请获得证书主体的有效合法授权。

3.1.3 注册过程与责任

（1）证书申请

申请人需首先根据证书应用项目、证书类别，按照 SZCA 服务指南/通知公告要求，向 SZCA 或 SZCA 授权注册机构提交证书申请资料。申请证书时，证书申请者必需保证提交的所有证书申请信息的真实准确合法有效，并接受、遵守 SZCA 的《电子认证服务协议》、CPS 或 CP，否则 SZCA 有权不予受理、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。且如证书申请者选择自行或委托第三方生成证书密钥对的，证书申请者应确保密钥对在安全的环境下生成、保存且申请者自始拥有对私钥的使用控制权。

（2）证书受理与注册

SZCA 及其授权注册机构受理证书申请时，应告知用户证书申请要求、证书用途功能、使用方式与法律风险，应根据本 CPS“2.2 身份标示与鉴别”相关规定，在授权范围内收集、审核用户证书申请，含证书申请资料的齐全性、填写的完整性规范性，及证书申请格式、证书申请资格和条件的符合性审核，对申请做出驳回和受理的决定。

申请一经受理，注册机构完成用户证书申请信息（含用户信息）系统注册录入，并将证书申请通过安全通道发送传递给 CA。且在受理证书申请后，应要求证书申请人同意接受《电子认证服务协议》并与 SZCA 签署该协议。RA 应保证证书申请和证书用户信息来源于证书申请人，递交给 CA 的证书申请人的信息完整未被篡改，且保证相关个人隐私信息的安全保密。

SZCA 按照法律法规、主管部门相关规定及 CPS、CPS 相关要求开展数字证书受理、审核及签发相关活动。SZCA 应保证注册的证书申请

人信息不被篡改、泄露或遗失、及免受不被授权的访问和使用。

SZCA 或授权注册为用户生成证书密钥对时，应保证密钥对安全生成并安全分发给证书申请人。

3.2 证书申请处理

3.2.1 执行识别与鉴别功能

SZCA 或授权的注册机构遵循本 CPS 第 2.2 章“2.2 身份标识与鉴别”的规定和相关流程，对证书申请者提交的申请材料进行审核，对证书申请者的身份进行鉴别。

3.2.2 证书申请批准和拒绝

SZCA 或其授权注册机构在完成全部证书申请鉴别流程后，根据鉴别结果，决定申请的批准或驳回

（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、批准证书申请，并提交证书请求后，SZCA 负责签发证书。

如批准申请的，SZCA 或其授权注册机构将保存归档相关证书申请、认证材料或信息。

（2）证书申请的驳回

SZCA 或其授权的注册机构根据其独立判断，有权拒绝证书申请，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或存在其他不符合申请条件的情形，SZCA 或其授权注册机构将驳回申请者的证书申请。

被拒绝的证书申请人可再次提出申请。

3.2.3 处理证书申请的时间

在提交的申请材料齐全并符合要求的情况下，SZCA 或授权的注册机构将在 5 个工作日内对证书申请者提交的申请信息进行审核，若情况特殊需延长，需通知申请人并说明理由。法律或监管政策另有规定的，依其规定执行。

3.2.4 告知证书申请的结果

拒绝证书申请的，SZCA 或授权的注册机构将在 5 个工作日内以适当的方式（如短信、电话、电子邮件、信函快递邮寄等）通知用户，并一并告知拒绝的理由，如用户没有提交所规定的文件；未通过身份信息鉴别和验证、未配合提交补充验证资料或未进行补充鉴别验证；用户没有在规定时间内回复通知；未缴纳证书费用等等。

3.3 证书签发

3.3.1 证书签发中注册机构和认证机构的行为

SZCA 或其授权的注册机构批准证书申请后，RA 将用户信息通过安全通道传输发送至 SZCA，SZCA 经验证注册机构的签名或注册机构的权限，确认 RA 的证书签发请求正确无误后，SZCA 通过证书签发系统签发证书，并将证书签发的信息通过适当的方式通知证书申请者或 RA。SZCA 注册机构负责将证书及证书口令、证书获取方式等提供、告知给用户。

3.3.2 认证机构和注册机构对用户的通告方式

SZCA 通知注册机构证书签发的方式，包括系统通知、消息、及其他可靠方式。SZCA 或注册机构通知订户证书签发的方式包括面对面、短信、电子邮件、电话、信函、系统消息及其他 SZCA 认为可行的合法方式。

3.3.3 证书获取方式

SZCA 或其注册机构提供的证书获取方式包括：

（1）提供证书下载渠道，包括短信、电子邮件、平台站内信等方式提供证书下载链接；

（2）交付含证书的证书介质，包括面对面、邮寄证书智能密码钥匙等；

（3）提供证书密码、激活数据，通过短信、电子邮件、平台站内信等方式提供证书密码、激活数据。

3.4 证书接受

3.4.1 构成接受证书的行为

在 SZCA 数字证书签发完成后，注册机构将数字证书及证书口令、证书获取方式等提供、告知给证书申请者。

接受证书的方式包括以下任一方式：受领证书介质、下载证书、获取或使用证书激活数据、获得或使用证书密码、使用证书、订户在收到或应当收到证书签发通知或证书后 2 日内未通知 SZCA 或其注册机构提出异议（无论用户实际是否下载、获取、使用证书），订户回复、通知收到、接受证书等。

3.4.2 认证机构对证书的发布

除非证书订户明确拒绝发布证书，或证书部分信息项，否则 SZCA 签发的证书将发布到 LDAP 目录服务器中。

3.5 密钥对和证书的使用

3.5.1 用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钥，避免遗失、泄漏、被篡改或非授权使用。订户应在法律法规、证书对应的 CPS、CP、服务协议及证书（如密钥用途、扩展密钥用途）要求允许的证书应用范围内按照约定的方式使用证书及其私钥。且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。否则造成的损失，由证书订户自行承担。

3.5.2 信赖方公钥和证书的使用

依赖方应按约定的方式，使用订户证书公钥验证证书及签名信息，且依赖范围应基于 CPS、CP 与证书内容规定的内容，依赖方接受数字签名信息时需要验证如下内容：

1) 获得数字签名对应的证书和信任链，确认该签名对应的证书是否是依赖方信任的证书，如是否由合法的 CA 签发。
2) 检查证书密钥用法、扩展密钥用法证书项，比对证书的实际用途是否符合证书内容规定的用法要求。

3) 使用证书上的公钥验证签名。

4) 确认数字签名对应的证书状态正常，证书在签名时处于有效期，没有进入 CRL 列表。

依赖方应使用接收方的公钥进行信息加密，公钥证书应同加密信息一同发送给接收方。

3.6 密钥更新

3.6.1 密钥更新的情形

密钥更新通常指密钥和证书同时更新，即证书申请人或其他参与者生成一对新密钥并申请为公钥签发一个新证书。被撤销的证书不能进行密钥更新和证书更新。

如出现下列情形的,订户必须选择证书密钥更新：

1) 证书或其密钥对即将到期；

2) 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；

3) 其他可能导致密钥更新的情形。

此外，凡是在 SZCA 运营体系架构内部使用的证书，包括 RA、管理员证书、审计员证书等证书，必须在到期前进行证书密钥更新。

3.6.2 证书更新的情形

证书更新通常是指密钥不变，证书有效期延长。证书更新业务规则参照密钥更新执行。

3.6.3 更新申请的提交

在订户的证书有效期届满前，SZCA 将做出合理的努力向证书订户或者授权委托人发送证书更新提示通知，方式包括但不限于提示消息、书面提示、电话通知、短信通知、电子邮件通知或其它方式，SZCA 和其授权的证书注册机构采取了上述通知方式中任何一项，均可被视为进行了合理的努力。订户可根据自身需要决定是否提出证书更新申请。

SZCA 在此提醒：订户在进行密钥更新或证书更新之前，应将原密钥加密过的文件进行解密，同时备份好解密文件，然后将证书删除。以上操作完成后才能进行密钥更新或证书更新。如订户未解密文件而进行

密钥更新或证书更新，由此造成的损失，SZCA 概不负责。

证书订户如需更新证书或更新证书密钥，必须在证书有效期届满前一个月内，到 SZCA 授权的注册机构申请更新证书。

证书持有者、证书持有者的授权代表（如：机构证书、机构个人证书、机构的设备证书等）或证书对应实体的拥有者（如设备证书等）可以提交密钥更新或证书更新，应提交身份证件影印材料，并签署《电子认证服务协议》。

3.6.4 更新申请的鉴别

参见本 CPS “2 身份标识与鉴别”的规定。处理密钥更新请求应对原证书、申请的签名信息及身份信息进行验证和鉴别，无误后方可进行。

3.6.5 密钥更新方式

SZCA 授权的注册机构对订户提交的密钥更新申请进行查验，详情参见本 CPS“2.2 身份标示与鉴别”和“2.3 密钥更新请求的标识与鉴别”规定。

证书密钥更新流程主要包括：

1) 注册机构审核通过后，提交申请至 SZCA；
2) SZCA 撤销旧证书，为订户更新密钥、签发新证书；
3) 注册机构为订户制作证书，将新证书及证书密码提供告知订户，并通知订户；
4) 新证书签发成功后，SZCA 将证书发布到 LDAP 目录服务器、证书撤销信息发布到 CRL。

3.6.6 通知证书持有者密钥更新

密钥更新后的新证书签发通知的时间和方式，执行参见本 CPS “3.3.2 认证机构和注册机构对用户的通告方式”。

3.6.7 构成接受密钥更新的行为

参见本 CPS “3.4.1 构成接受证书的行为”。

3.6.8 认证机构对密钥更新的发布

参见本 CPS“3.4.2 认证机构对证书的发布”。

3.7 证书变更

3.7.1 证书变更的情形

当证书中除订户公钥之外的订户身份或者属性信息发生变化时，如订户姓名、名称、住所地、隶属的组织或部门、岗位、角色等变更导致 DN 项或改变，订户应向 SZCA 申请对已签发的数字证书进行证书变更。SZCA 将为用户签发新证书，同时将撤销原证书。

3.7.2 证书变更的申请

证书主体申请的主体，同本 CPS“3.6.3 更新申请的提交”规定，即已经申请并持有使用 SZCA 证书的实体，或其授权经办人可提出证书变更申请。

3.7.3 证书变更的鉴别

参见本 CPS “2.2 身份标示与鉴别”的规定。

3.7.4 证书变更受理方式

证书变更业务的操作流程，按照证书申请的受理流程，执行参照本 CPS 第 3.1、3.2 章节规定。

3.7.5 通知证书持有者证书变更

参见本 CPS“3.3.2 认证机构和注册机构对用户的通告方式”规定。

3.7.6 构成接受证书变更的行为

参见本 CPS “3.4.1 构成接受证书的行为”规定。

3.7.7 认证机构对证书变更的发布

参见本 CPS“3.4.2 认证机构对证书的发布”。

3.8 证书撤销

3.8.1 证书撤销的情形

SZCA、注册机构及证书持有者在发生下列情形之一时，应申请撤销数字证书：

1) 政务机构的证书持有者不从事原岗位工作；
2) 司法机构要求撤销证书持有者证书；
3) 证书持有者提供的信息不真实；
4) 证书持有者没有或无法履行有关规定和义务；
5) 认证机构、注册机构或最终证书持有者有理由相信或强烈怀疑一个证书持有者的私钥安全已经受到损害；
6) 政务机构有理由相信或强烈怀疑其下属机构证书、人员证书或设备证书的私钥安全已经受到损害；
7) 与证书持有者达成的服务协议已经终止；
8) 证书持有者请求撤销其证书；
9) 法律、行政法规规定的其他情形。

3.8.2 可以发起请求撤销证书的实体

证书持有者、证书持有者所属的组织机构或证书使用唯一依赖方、SZCA 及其注册机构，发现出现符合证书撤销条件中的情形时，均有权发起证书撤销申请。

3.8.3 证书撤销的申请

SZCA 在此提醒：订户在进行证书撤销之前，如需使用原证书加密的文件，应在申请证书撤销前，将原密钥加密过的文件进行解密，同时备份好解密文件。以上操作完成后才能进行证书撤销申请、删除证书。否则由此造成的损失，SZCA 概不负责。

申请者提交身份证件、填写签署《电子认证服务协议》等申请资料，注明申请撤销的原因，向 SZCA 及其授权的注册机构递交证书撤销请求。

3.8.4 证书撤销的鉴别

认证机构、注册机构在接到证书持有者的撤销请求后，应对其身份

进行鉴别并确认其为证书持有者本人或得到了证书持有者的授权，鉴别流程参见本 CPS “2.2 身份标示与鉴别”、“2.4 撤销请求的标识与鉴别”规定。

3.8.5 证书撤销受理方式

参见本 CPS “3.1.1 证书申请流程”规定，包括线下、线上方式，情况紧急的，可电话联系通知 SZCA 或其注册机构。

3.8.6 认证机构处理撤销请求的时限

SZCA 及其授权注册机构在接到客户撤销请求后，符合撤销条件的，24 小时内能够完成证书撤销流程，并在 CRL 上公布撤销的证书信息。

3.8.7 通知证书持有者证书撤销

参见本 CPS “3.3.2 认证机构和注册机构对用户的通告方式”。

3.8.8 构成接受证书撤销的行为

参见本 CPS “3.4.1 构成接受证书的行为”。

3.8.9 认证机构对证书撤销的发布

SZCA 将撤销的证书信息写入 CRL 列表并签发公告最新的 CRL，也可以通过官网、公众号等方式发布证书撤销信息。

3.8.10 CRL 发布频率

SZCA 证书撤销列表在 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。

3.8.11 CRL 发布的最大滞后时间

证书从撤销到发布到 CRL 上的滞后时间不得超过 24 小时。

3.8.12 在线状态查询的可用性

SZCA 提供证书状态的在线查询服务（OCSP），该服务 7X24 小时可获得。

3.8.13 在线状态查询要求

SZCA OCSP 系统查询没有设置任何读取权限。已归档的订户证书，SZCA 有权限制 OCSP 的访问权限。

3.9 密钥生成、备份与恢复

3.9.1 证书持有者密钥恢复

证书加密密钥对的生成、备份和恢复应由国家密码管理局和省部密码管理部门规划建设的密钥管理基础设施提供密钥管理服务。

密钥恢复按照证书申请的身份鉴别与受理流程执行，将加密证书的归档或备份密钥，恢复到可用状态。

3.9.2 问责取证密钥恢复

国家司法机关、行政执法机构或主管部门因执法、司法或行政管理取证的需要，需要恢复加密密钥的，应遵照国家相关法律规定的程序向 SZCA 提出申请。

4 应用集成支持与信息服务操作规则

4.1 服务策略和流程

1. SZCA 在与客户签署合同时，项目管理团队负责进行项目立项，制定证书应用实施的管理策略和流程，对业务系统进行充分调研，指导或参与业务系统证书应用部分的开发和实施；

2. 项目管理团队、技术开发团队制定项目管理制度、产品研发管理制度，规范系统和程序开发行为；

3. 技术开发团队制定安全控制流程，明确人员职责；

4. 技术开发团队实施证书软件发布版本管理，并进行证书应用环境控制；

5. 项目开发程序和文档等资料项目管理团队、技术开发团队应妥善归档保存。

4.2 应用接口

4.2.1 密码设备调用接口

密码设备应用接口应包括服务器端密码设备的底层应用接口和客户端证书介质（如：USBKey）的底层应用接口。

服务器端密码设备的底层应用接口符合 GM/T 0018 的要求；客户端证书介质的底层应用接口符合 GM/T 0016 和 GM/T 0017 的要求。

4.2.2 密码模块安全技术接口

密码模块安全技术接口，符合 GM/T 0028 和 GM/T 0054 的要求。

4.2.3 通用密码服务接口

通用密码服务接口为各类密码服务层和应用层提供统一的通用密码服务接口，符合 GM/T 0019 的要求。

SZCA 提供证书应用接口程序供应用系统集成和调用。

4.3 集成内容

SZCA 应为电子政务应用单位提供证书应用接口程序集成工作。集成工作应提供以下服务：

(1) 证书应用接口的开发包（包括客户端和服务器端）；
(2) 接口说明文档；
(3) 集成演示 Demo；
(4) 集成手册；
(5) 证书应用接口开发培训和集成技术支持；
(6) 协助应用系统开发商完成联调测试工作。

4.4 信息服务内容

4.4.1 证书信息服务

SZCA 可根据电子政务证书应用单位对证书应用信息的管理及决策需求，根据合同约定或政府单位书面要求，通过书面汇报证书应用情况，或系统对接接口同步证书信息等方式，提供证书信息以供管理决策。

4.4.2 CRL 信息服务

所有被撤销或挂起的证书，写入列表 CRL 自动发布，通过 SZCA 的 LDAP 目录服务器发布，如需要，SZCA 可按照合同根据合同约定或政府单位书面要求，将特定项目特定范围的证书的 CRL 同步到政府单位的信息系统。

4.4.3 服务支持信息服务

SZCA 为证书应用对外发布提供证书驱动、证书应用接口及其开发文档、证书安装使用指南、证书常用问题解答、CPS 等，以支持应用系统集成商、开发商及电子政务订户、依赖方的证书应用。

4.4.4 决策支持信息服务

对司法机关、行政管理部门、主管部门、电子政务应用单位因司法、决策、行政管理需要提出的取证、调研需求，包括用户档案信息、投诉处理信息、用户满意度信息、服务效率信息、CA 业务运营调研材料等，SZCA 将依法配合提供。

4.5 信息服务管理规则

SZCA 在提供信息服务时，将按照《个人信息保护政策》《数据安全

管理办法》《商业秘密保护管理办法》《协助调查取证管理办法》《协助调查取证工作细则》做好相关信息的隐私保障机制，实现对用户的信息保护承诺。

（1）私有信息的收集使用

SZCA 仅允许在进行证书发放和管理时才能收集 CPS 声明的私有信息。除了已与用户沟通确认或取得用户同意外，CA 或 RA 不应收集更多私有信息。因在某项业务中开展证书应用而获得的私有信息，在使用时将获得该业务应用单位的许可。

SZCA 应采取安全手段对用户私有信息进行安全存储，确保用户私有信息不发生泄露、未授权访问等安全事件。

（2）私有信息的发布与提供

SZCA 和注册机构仅能面向证书应用单位发布与之相关的私有信息，以协助证书应用单位进行证书业务管理，且一般证书应用单位的信息访问权限仅限于该应用业务系统内涉及的证书。任何特定的私有信息发布应遵照相关法律和政策实行。

SZCA 或者注册机构在以下情况下，可以执行将私有信息提供获得相应授权的人员：

1) 司法程序；
2) 经私有信息所有者同意；
3) 按照明确的法定权限的要求或许可。

同时 SZCA 将执行以下信息服务管理规则：

a) 对 CA 机构内的工作人员按其工作角色设定与之相应的信息访问权限，并对其所有访问操作进行详细记录。
b) 对证书应用单位的管理员设定信息访问权限，限定其仅能访问本应用所签发证书信息。
c) 对问责取证程序需要进行的信息访问，应严格审核相应的问责人员身份及授权文件，无误后方可进行问责取证。
d) 对监管部门应管理需求进行的信息访问，应按照相关的管理规定和调取程序，为其提供信息访问权限。

4.6 信息服务方式

4.6.1 证书信息同步服务

证书信息同步服务可采用接口技术实现 CA 系统与电子政务信息系统的证书应用同步。电子政务信息系统通过部署统一的接口，认证机构的 CA 系统通过调用统一的同步接口，实现 CA 系统向电子政务信息系统进行证书信息的自动同步功能。同时，为了保证数据传输的安全性，可通过对通信数据添加数字签名，以防止数据在传输中被篡改或损坏。

4.6.2 CRL 信息同步服务

CRL 信息同步服务可采用技术实现 CA 系统与电子政务信息系统的 CRL 同步。

为了提高 CRL 文件传输的安全性，应对发送的 CRL 数据进行数字签名，电子政务信息系统只需要根据认证机构身份标识找到对应的根证书链，验证 CRL 签名的有效性即可确定 CRL 的有效性。

CRL 发布周期不得超过 24 小时。

4.6.3 服务支持信息服务

SZCA 通过 WEB 网站等面向电子政务用户发布如下信息：

a) 电子政务电子认证服务业务规则；
b) 证书生命周期服务流程及相关费用；
c) 证书用户操作手册；
d) 证书常见问题解答（FAQ）；
e) 获得证书帮助联系方式（用户服务方式、办公地址、邮政编码、投诉电话等）；
f) 其他应该发布的相关信息。

SZCA 通过 WEB 网站面向电子政务应用系统集成商发布如下信息：

a) 数字证书应用接口软件包；
b) 数字证书应用接口实施指南；
c) 证书常见问题解答（FAQ）；
d) 获得证书帮助联系方式（用户服务方式、办公地址、邮政编码、投诉电话等）；

e) 其他应该发布的相关信息。

SZCA 通过 WEB 网站面向电子政务应用系统发布如下信息：

a) 时间戳服务数据接口；
b) HTTP 协议的 CRL 发布服务接口；
c) LDAP 协议的 CRL 发布接口；
d) LDAP 协议的证书发布接口；
e) OCSP 服务接口。

4.6.4 决策支持信息服务

SZCA 面向证书应用单位以接口等方式提供如下信息服务：

A.用户档案信息：分业务、地域、时段等要素提供用户信息的统计分析服务；

B.投诉处理信息：提供特定业务、时间、特定用户群、问题类型等的投诉处理汇总信息及分析；

C.用户满意度信息：提供面向业务的用户满意度调查信息；

D.服务效率信息：提供面向业务的服务效率分析信息，如处理时间、服务接通率等。

5 使用支持服务操作规则

5.1 服务内容

5.1.1 面向证书持有者的服务支持

A.数字证书管理

包括数字证书的导入、导出，以及客户端证书管理工具的安装、使用、卸载等。

B.数字证书应用

基于数字证书的身份认证、电子签名、加解密等应用过程中出现的各种异常问题，如：证书无法读取、签名失败、证书验证失败等。

C.证书存储介质硬件设备使用

包括证书存储介质使用过程中出现的口令锁死、驱动安装、介质异常等。

D.电子认证服务支撑平台使用

为用户提供在认证机构的数字证书在线服务平台中使用的各类问题，如：密钥更新失败、下载异常、无法提交注销申请等。

5.1.2 面向应用提供方的服务支持

A.电子认证软件系统使用

提供受理点系统、注册中心系统、LDAP、OCSP、信息服务系统等系统的使用支持问题，如证书信息无法查询、数据同步失败、服务无响应等。

B.电子签名服务中间件的应用

解决服务中间件在集成时出现的各种情况，如客户端平台适应性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等。

5.2 服务方式

5.2.1 座席服务

用户拨打 SZCA 的服务热线 400-112-3838，通过语音系统咨询证书应用问题，热线座席根据用户的问题请求，查询系统知识库清单，协助用户处理。

5.2.2 在线服务

SZCA 在线服务通过提供自助信息查询系统、网络实时通讯系统、远程终端协助系统，以及在线帮助与传统模式（电话服务）的结合，满足用户多种服务帮助的需求。

5.2.3 现场服务

SZCA 根据用户的实际需求，由技术支持工程师上门现场为用户处理数字证书应用中存在的问题。

5.2.4 满意度调查

通过多种用户可接受的调查方式进行用户回访，包括电话、WEB 网站、邮件系统、短信、传真等。

向用户提供调查表格以供用户填写，调查表格应清晰载明此次回访的目的及内容，并将用户回访中产生的相关文档进行归档、保存。

5.2.5 投诉受理

SZCA 可通过电话、网站平台、电子邮件、即时通讯工具等方式及时接受用户投诉，投诉受理过程中应记录投诉问题，并将结果及时反馈给用户。并将投诉受理中产生的相关文档进行归档、保存。

5.2.6 培训

培训方式可以由 SZCA 与用户双方约定的形式开展。

培训内容主要包括：电子认证服务基础性技术知识、服务规范、证书应用集成规范及相关帮助文档、常见问题解答（FAQ）、操作手册等。

5.3 服务质量

座席服务、在线服务、现场服务时间应充分满足各类用户的需要，至少为 5×8 小时工作时间。在有应急服务需求的特殊情况下，服务时间应根据具体业务需求确定，甚至是 7×24 小时不间断服务。

SZCA 对技术问题和技术故障按照一般事件、严重事件、重大事件进行分类，并制定响应处理流程和机制，以确保服务的及时性和连续性。技术支持响应时间应以最大程度不影响用户使用为准则。

6 认证机构设施、管理和操作控制

6.1 物理控制

6.1.1 场所区域与建筑物

SZCA 认证系统的机房位于深圳市龙华区观澜街道库坑社区龙华大道泗黎段 402 号的 1 号楼 3 楼。机房按功能分为 CA 管理区、CA 服务区、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。

6.1.2 物理访问

操作人员进入机房，必须通过 IC 卡门禁系统和密码系统的身份检验，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，必须通过该区域密码和权限检验，并且所有的操作过程都进行记录。

6.1.3 电力和空调

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。

6.1.4 水患防治

SZCA 的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。

6.1.5 火灾预防和保护

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。

6.1.6 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。

6.1.7 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，所有的销毁行为遵守我国有关的法律法规。

6.1.8 异地备份

暂无，SZCA 后将视情况对重要数据进行异地备份。

6.1.9 入侵侦测报警系统

在机房场所建筑区域内安装入侵侦测报警系统，发生非法入侵能及时报警。

6.2 操作过程控制

6.2.1 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 安全策略管理委员会
- 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。

6.2.2 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。

6.2.3 角色职责分离设置

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。

6.3 人员控制

6.3.1 可信人员要求

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。

6.3.2 可信人员背景审查

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。应聘人员提供以下资料：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)人事部门可自行或委托第三方背调机构通过电话、网络、信函或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。

SZCA 有权视员工的工作性质、岗位关键重要程度等情况，决定与员工签订并执行保密协议、竞业协议，要求相应员工在劳动合同关系存续期间或员工离职后的规定时间仍然不得从事与 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，被通知执行竞业协议的员工在离职后的规定期间仍然不得从事与 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。

6.3.3 人员培训及再培训

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：

（a） 公司文化及各类管理制度；

（b） 安全管理制度；

（c） 专业知识培训；

（d） 岗位职责及岗位技能培训；

（e） 相关法律、管理办法等。

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。

6.3.4 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。

6.3.5 违规行为处罚

当 SZCA 员工进行了未授权或越权操作或对系统的未授权使用，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，按照内部规章制度进行处理，构成犯罪的提交司法机关处理。

6.3.6 外包服务人员及要求

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。

6.3.7 提供给员工的文档及保密策略

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 电子政务电子认证业务规则；
(3) SZCA 技术体系文档；
(4) SZCA 安全管理制度；
(5) 其他工作必需的文档。

6.4 审计日志程序

6.4.1 审计日志定义

审计日志，是记录 SZCA 的物理环境、CA、KM、RA 系统运行、配套设备安装维护、密钥和证书生命周期管理、证书签发和 CLR 生成、PKI 系统访问操作、人员机房和 PKI 系统操作、关键业务系统和数据库运行等相关的事件产生的日志。审计日志一般应包含事件日期、内容、发生时间段、相关实体。

6.4.2 审计日志安全检查与风险评估

SZCA 的超级管理员、系统审计员需要定期对安全策略和操作流程的执行情况进行检查确认，进行运营风险评估。

6.4.3 审计日志记录要求

SZCA 的审计日志应准确完整地记录 CA 机构涉及运营条件和环境、密钥和证书生命周期管理的日志和事件。

6.4.4 审计日志处理或归档周期

各类日志、安全事件的记录应在安全和公正的情况下以自动或手动方式产生，并定期归档。授权安全管理人员定期检阅记录和跟进有关事项。SZCA 每月对记录进行审查，对审查记录行为备案。

6.4.5 审计日志检测系统

SZCA 建立监测 CA 系统访问的检测系统或安全机制，保证非授权的访问能够被发现。

6.5 规定事件记录的类型

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) 注册系统和证书受理操作的相关授权记录及管理记录；

(2) 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；

(3) 密码设备生命周期管理

(4) 证书生命周期的各项操作，包括证书申请、证书密钥更新、证书变更、证书撤销等事件；

(5) 证书签发和 CRL 列表生成；

(6) PKI 系统访问；

(7) 操作 PKI 系统和其他安全系统的行为；

(8) 安全配置文件变更；

(9) 系统崩溃、硬件故障和其他异常；

(10)防火墙和路由器的工作情况，机房进出访问等等。

(11)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；

(12)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；

(13)系统巡检记录；

(14)人员访问控制记录。

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。

6.6 规定事件记录的内容

事件记录，无论是手写、书面或电子文档形式，都包含事件类型、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。

6.7 记录归档要求

6.7.1 记录归档的保存期限

归档记录，包括但不限于所有审计数据、证书申请信息、支持证书

申请的文档、证书申请审批资料、证书及 CRL 等类型的资料。SZCA 电子政务电子认证服务归档记录保存期限为证书失效后 5 年。

6.7.2 记录归档的保护措施

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。

6.7.3 记录归档的备份程序

所有存档文件的数据库保存在 SZCA 的存储库中，并将进行备份。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。

6.7.4 记录归档时间戳要求

暂无。

6.7.5 记录归档收集系统

SZCA 档案的收集系统由人工操作和应用程序、网络、操作系统自动操作两部分组成。

6.7.6 记录归档检验机制

SZCA 定期验证存档信息的完整性。

6.8 认证机构密钥更替

当 CA 根密钥对累计寿命超过本 CPS “7.3.2 证书操作期和密钥对使用期限”中规定的最大有效期时，SZCA 将启动密钥更新流程。密钥更替时 SZCA 采用与初始化根密钥相同的方式进行。旧的 CA 密钥对到期前，SZCA 将用新的 CA 密钥对签发证书。

6.9 数据备份

6.9.1 数据备份计划

SZCA 制定的数据备份计划，包括数据备份的内容、周期、备份方式，并将根据备份策略定期对系统、数据库、CRL、系统日志等进行备份。

6.9.2 异地备份中心

SZCA 制定容灾备份恢复计划和应急响应预案等。并将根据业务需要，选择建立同城容灾备份系统或异地容灾备份系统。

6.10 损害与灾难恢复

6.10.1 事件和损害的列表

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 应急相关制度、流程、方案进行处理，必要时启动备份系统。

6.10.2 计算资源、软件或数据的损坏

当认证系统运营使用的系统、网络、软件、数据库数据、根证书密钥或者其它信息出现异常损毁时，可以依照 SZCA 灾难恢复相关制度规定的流程、方案、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。

6.10.3 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 将启用 SZCA 根私钥泄露紧急处理流程进行处理，包括但不限于向主管部门报告、对泄密证书进行冻结吊销处理，新生成根证书。

6.10.4 灾难后的业务连续性能力

SZCA 在遭遇本 CPS“6.10.1 事件和损害的列表”、“ 6.10.2 计算资

源、软件或数据的损坏”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。

6.10.5 业务连续性计划

SZCA 制定的业务可持续性计划，并进行定期检查和更新，确保其持续有效。

6.11 认证机构或注册机构的终止

当 SZCA 及其授权注册机构需要终止经营时，将会按照《电子签名法》《电子政务电子认证服务管理办法》等法律法规之规定执行，在终止服务前向国家密码管理部门报告，通知订户、依赖方及其他相关当事方，并与其他电子政务电子认证服务机构自主协商或向国密局申请就业务承接做出妥善安排。

7 认证系统技术安全控制规则

7.1 密钥对的生成和安装

7.1.1 密钥对的生成

1.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。

2.签名密钥对：

通常证书订户的签名密钥对由用户端产生，证书申请者可使用国家密码管理局认可批准的、SZCA 数字证书签发系统支持的硬件或软件（商用密码软件模块）生成签名密钥对。签名密钥存储在介质中不可导出，无法被复制。

选择密钥协同证书的，订户的签名密钥，是由用户端与服务端协同密码服务器各自生成密钥分量，由用户控制进行协同签名的证书类型，SZCA、用户共同保障订户密钥安全。

7.1.2 私钥传送给用户

通常，订户证书的签名密钥对由用户自己生成并保管。密钥协同签名证书，订户的签名密钥对由用户端与服务端协同密码服务器各自生成密钥分量。签名私钥由订户自己生成时不需要传送。

用户如委托 SZCA 产生密钥时，SZCA 将以用物理的方式传递私钥、邮寄保存私钥的令牌、或是通过 SSL 会话传递私钥等安全方式将私钥传送给用户，并确保私钥在交付用户前未被使用。

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。

7.1.3 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。SZCA 通过在线 SSL 会话或经注册机构签署的消息将订户签名证书公钥安全地提供给注册机构。

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。

7.1.4 认证机构公钥传送给依赖方

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

7.1.5 密钥的算法

密钥算法符合国家密码管理局认可的算法。SZCA 签发的订户证书的密钥对长度支持为 RSA 1024 位、2048 位及 SM2 256 位及以上，以及国家密码管理局要求的密钥长度。且 SZCA 不推荐订户使用或订户申请签发 RSA 1024 位密钥对的数字证书。

7.1.6 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。

7.1.7 密钥使用目的

证书持有者的密钥对和证书应当用于其规定的、批准的用途。签名密钥对用于签名与签名验证，实现身份认证、不可抵赖性和信息的完整性等；加密密钥对用于加密解密。如果密钥对允许用于身份鉴别，则可以用于身份鉴别。密钥对和证书不应用于其规定的、批准的用途之外的目的，否则其应用不受保障。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。

7.2 私钥保护和密码模块工程控制

7.2.1 在 CA 私钥保护方面的要求

SZCA 的 CA 系统使用国家密码主管部门批准使用的符合国家标准的许可的密码模块产品（加密机），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。

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。对加密机中的密钥进行操作，必须由 2 位或以上具备权限的密钥管理人员和操作人员共同现场完成，任何人无法独立完成操作。

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。

7.2.2 用户私钥保护方面的要求

电子政务的证书应用，数字证书对应私钥，订户通过密码设备生成的签名私钥不可导出密码模块。订户私钥在硬件密码设备或密码模块中加密保存。签名密钥对为证书持有者专有，生成、存储和使用受证书持有者安全管控。

加密密钥对由国家密码管理局和省部密码管理部门规划建设的密钥管理基础设施提供密钥管理服务。

7.3 密钥对管理的其他方面

7.3.1 公钥归档

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

7.3.2 证书操作期和密钥对使用期限

订户证书有效期通常不得超过 5 年，订户密钥有效期与其证书有效期相同。

1. 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。

2. 对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公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加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

3. 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。

4. 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。

SZCA 根证书有效期为 20 年、30 年。

7.4 激活数据

7.4.1 激活数据的产生和安装

用于保护存放有认证机构 CA 私钥的密码设备激活信息（秘密分割）的产生过程必须安全可靠，符合密钥激活数据分割和密钥管理办法相应的安全要求。秘密分割的创建和分发记录有相应的日志。

7.4.2 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，如使用口令、PIN 码，订户必须进行妥善的保管，防止泄漏或窃取。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：USB 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。如果证书持有者使用生物特征保护私钥，证书持有者也应注意防止其生物特征被人非法获取。

7.4.3 激活数据的其他方面

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。

当私钥的激活数据进行传送时，应保护它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。还有，Windows 或网络的登录用户的用户名/密码（用于证书持有者激活数据），经过网络传送时注意非法用户的窃取。

7.5 系统安全控制

7.5.1 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、访问认证系统服务器；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，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。系统口令必须符合口令安全管理要求。

7.5.2 安全技术措施

SZCA 的 CA 认证系统的需通过国家密码管理局的安全性审查和互联互通测试，建设需符合相关标准规范，相关密码设备具备国家密码管理局颁发的商用密码产认证资质。

7.6 生命周期技术控制

7.6.1 CA 系统运行管理

CA 系统的操作应按规定的操作流程进行。CA 系统（包括软件、网络等方面）的变更需经管理层批准，经批准的变更实行前必须通过测试，并进行记录。可能对系统的安全性有影响的改动必须事先进行风险评估，改动前应进行备份并得到管理层的明确批准。

CA 中心的测试系统、运营系统、网络设施等，具有专门的操作维护人员，并有相应明确的授权。SZCA 操作维护人员需要定期检查系统及网络的稳定性、安全性及容量，确定符合服务水平。

SZCA 建立检测和防护控制来防止病毒和恶意软件，并能提供适当的报警信息。SZCA 建立监控流程，确保记录并报告发现的或怀疑的、

对系统或服务有威胁的安全缺陷。建立并执行系统故障报告、处理流程。

SZCA 建立制度，对 CA 系统相关的媒介（包括设备、证书介质、文档等）进行妥善保管，避免非授权的访问。

7.6.2 CA 系统访问管理

SZCA 制定 CA 系统的访问策略。

SZCA 制定 CA 系统访问人员角色职能定义，确保合理的职责分割和权限控制，并明确授权及取消授权的操作流程和策略。

SZCA 制定网络安全策略，并制定访问网络的控制策略。

SZCA 制定操作系统及 CA 软件的安全访问的策略。

SZCA 建立各种对 CA 系统访问的审计措施。

7.6.3 CA 系统的开发和维护

SZCA 的系统具有国家密码管理局批准认可的商用密码产品认证证书资质，并由生产商按照国家相关的安全标准开发。

SZCA 的 CA 系统配置、升级更新、源代码访问、新增或修改软件都会记录在案并进行流程控制、测试、检查、访问控制等管理，以防止未授权的修改。

7.7 网络的安全控制

SZCA 有防火墙、入侵检测、防病毒、安全身份认证等安全技术，如只有经过授权的 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，确保认证系统安全运营。

对于认证系统的网络安全，应制定相应的网络安全策略与管理制度。

7.8 时间戳

SZCA 部署时间戳系统，在系统关键业务运行日志、操作日志等日志中，保证可以使用时间戳服务。

8 法律责任和其他业务条款

8.1 费用

8.1.1 免费或收费策略

SZCA 的证书相关服务采取市场化定价策略。具体收费项目及相应收费标准视市场需求、项目情况、业务成本等多方面因素而定，且 SZCA 有权根据需要调整。各地政府部门对电子政务电子认证服务的收费政策有特别规定的（如涉企收费），SZCA 按当地政策执行。

证书相关服务费用在 SZCA 官网 https://www.szca.com 或其他 SZCA 服务平台上公布。如 SZCA 与订户、SZCA 与合作方对于证书服务费用另有书面约定的，以书面约定的价格为准。证书服务收费标准，按 SZCA 明确指定的时间生效，若未指定生效时间的，自公布之日起生效。SZCA 也可以通过其它方法通知订户或其它各方费用变化。

注册机构直接面向用户收取证书费用的，应遵循合法、公平、合理原则，不得以 SZCA 的名义擅自增加收费项目或收取无关的费用。

SZCA 签发的电子政务电子签名证书，非因产品质量、功能、性能问题，有以下任一情形的，SZCA 或其注册机构不接受证书退款：

(1) 用户知悉或可能知悉证书签发之日起 3 日内未提出异议；

(2) 用户获取接受证书（含收到证书介质、证书下载渠道、或证书密码等）之日起 3 日内未提出异议；

(3) 用户知悉或可能知悉证书发布之日起 3 日内未提出异议。

如用户在规定的退款时间（证书签发后 3 日内）按照 SZCA 退款流程提出证书服务退款申请，SZCA 经审查符合以下全部退款条件的，将在审查通过后 15 个工作日内予以退款：

(1) 退款不存在任一不允许退款的情形；

(2) 证书及证书介质全新未使用。

用户有证据能够证明 SZCA 签发数字证书违反法律法规、本 CPS 导致数字证书或其电子签名无效，或证书有质量、功能问题无法正常使用，用户可在收到证书后 7 日内向 SZCA 提出退款申请，SZCA 经核实属实后，将 15 个工作日内予以退款。

8.1.2 证书签发和密钥更新费用

证书新办、证书密钥更新（含证书更新）、证书变更等涉及证书新签发的证书服务，SZCA 将收取证书费用。

8.1.3 其他服务费用

证书签署、数字证书及电子签名验证服务，SZCA 有权将其列为收费服务项目，具体费用标准依客户需求、服务性质等项目情况为定。

证书撤销、**证书解锁**、证书查询访问、证书吊销查询访问或证书状态查询、CPS 或 CP 的访问获取，SZCA 无偿提供服务，且服务方式仅限远程、电话或在线方式，服务不涉及提供任何有形物质载体（含纸质文件）；如客户针对前述无偿服务在其通常服务条件、方式之外提出更多要求，例如提出打印复印等文印服务需求，或要求邮寄快递，或提出其他定制化的服务需求，SZCA 有权适当收取相应费用。

8.2 财务责任

8.2.1 责任担保范围

SZCA 根据业务发展情况决定其投保策略，保险的责任担保范围以相关保险法律法规及保险合同约定为准。

8.2.2 责任赔付声明

根据《中华人民共和国电子签名法》《商用密码管理条例》《电子政务电子认证服务管理办法》相关法律法规规定，SZCA 对于订户、依赖方由于直接信赖 SZCA 的数字证书或电子签名开展电子政务业务活动因 SZCA 原因而遭受的实际损失承担赔偿责任，且赔付的前提是 SZCA 无法证明对订户或依赖方所遭受的损失无过错。SZCA 赔付范围不包括声誉损失、名誉损失、利润损失、可得利益损失、第三方损失或赔偿等间接损失或可信赖利益损失，除非经法院或仲裁机构裁判确认支持。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 CPS“ 8.8 偿付责任限制”。

因授权注册机构原因造成的订户或依赖方的经济损失，注册机构应承担赔付责任；SZCA 代为赔付后，有权向注册机构追偿。

8.3 业务信息保密

8.3.1 保密信息范围

保密信息包括但不限于以下内容：

（1)SZCA 及其注册机构的证书私钥，SZCA 证书认证系统或密钥管理系统或其他重要系统设备的密钥；

（2)SZCA 的商业战略、商业计划，人事档案，资产设备资料，财务报表、财务审计报告，销售方案、营销推广计划、客户清单、项目报价、产品定价，产品研发文件、产品配方、工艺流程、技术参数、配置参数等；

（3)SZCA 未公开的业务流程、业务模式、服务方案、技术方案、业务规范、业务标准、业务诀窍、技术方案与技术措施，含 SZCA 与注册机构之间未公开的业务流程、业务逻辑、服务方案、业务方案、业务分工；

（4)SZCA 系统架构、应用系统配置、系统运营维护流程与规范、安全策略（含物理环境、信息系统、密钥管理等安全策略）与安全措施、灾备计划、灾难恢复计划、应急响应计划、应急方案、业务连续性计划等文件；

（5)SZCA 运营管理信息，包括但不限于证书发证数据、客户资料档案、客户身份鉴证方案或策略、证书认证服务流程与规范、客户服务流程与规范、业务运营管理体系等；

（6)SZCA 与注册机构之间、SZCA 或注册机构与订户、依赖方或其他证书参与方之间、SZCA 与其他业务关联方之间的合同/协议、备忘录、通知、承诺函、往来函、通信邮件等；

（7)SZCA 或 SZCA 对注册机构的审计报告（含审计内容、结果)、合规评估报告、稽核检查报告等；

（8)SZCA 的监管报告、报备、汇报、请示等资料；

（9)订户申请资料信息、订户资料原始档案、电子化档案、订户身份标识鉴别信息等订户个人信息（含个人隐私信息）

（10)商业机密

（11)政府部门的敏感信息和工作秘密；

（12)与证书持有者证书公钥配对的私钥；

(13)证书申请与应用过程中的计算机、设备、信息系统、网络信息。

(14)其他根据信息性质、保密技术措施等可认定为保密信息的。

8.3.2 不属于保密的信息

1. SZCA 公开的证书办理条件、要求与流程，证书办理或操作使用指南；
2. SZCA 公开的证书办理资料模板，含电子认证服务协议、依赖方信息、或其他服务协议等通用协议模板；
3. SZCA 服务规范，如证书策略（CP）、电子认证业务规则（CPS）、个人信息保护政策；
4. SZCA 对外公开的服务流程与规范、项目解决方案、产品介绍信息、产品应用案例；
5. SZCA 发布的业务通知与公告，含价目表或收费标准；
6. 证书持有者证书中的公钥、经用户同意发布的公钥证书；
7. 证书状态及撤销列表信息（CRL）；
8. 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，但并不意味着将前述信息的知识产权或所有权转移给第三方或授权第三人任意使用、传播、修改，SZCA 和相应信息的所有人保留所有这些信息的知识产权或所有权。未经 SZCA 或信息的权利人同意，第三方不得传播、使用、修改非保密信息。

8.3.3 保护保密信息的责任

保密信息，除非法律法规规定或司法机关、行政执法部门、监管单位依法定程序要求或命令提供、披露的，SZCA 或其注册机构没有义务也不会对外公布、披露、提供或分享。这种依法进行的信息披露不被视为违反保密的要求和义务。

客户或其他参与方的保密信息，SZCA 或其注册机构将按照法律法规规定及披露方或数据主体的授权、指令处理相关保密信息，在未征得披露方或数据主体事先书面同意前不会对外泄露、提供、发布，或超出约定范围使用，或委托第三方处理其数据。其中证书订户个人信息的保密，见本 CPS 第 8.4 章的规定。

当披露方或数据主体要求 SZCA 公开或向第三方提供其保密信息的，应以书面方式给予 SZCA 授权，SZCA 将按照法律法规允许的方式进行

信息公开或提供，对披露保密信息引发的侵权或其他法律责任（含经济损失赔偿），由数据主体或披露方承担，与 SZCA 无关。

8.4 个人隐私保密

8.4.1 保护隐私的责任

SZCA、注册机构或其他相关参与方，对工作中知悉、获取的订户、依赖方等的个人隐私信息承担保密责任，应依法采取相应的技术措施和其他必要措施保护有关信息和数据安全，确保用户隐私信息不发生泄露、篡改、未授权访问等安全事件。

8.4.2 使用隐私信息的告知与同意

在电子政务电子认证业务中获得的订户隐私信息（含 CA、RA 收集的信息），SZCA 将仅用于证书签发(含身份标识与鉴别)、证书发布、及提供证书查询、证书状态查询、证书应用技术支持等证书生命周期管理服务，且将按照法律法规规定保存订户证书认证相关档案资料信息。且 SZCA 或其授权注册机构将按照我国适用的法律法规的规定，在办理电子政务电子认证业务时履行必要的告知及取得同意的法律义务。

SZCA 或其授权注册机构如需超出约定或授权同意范围使用、处理订户隐私信息，在处理前应另行征得订户的同意。未经订户同意，不得将订户隐私信息对外进行披露、共享、提供、发布、公开或传输至境外，除非法律法规规定无需取得用户同意。

电子政务电子认证服务涉及的个人隐私信息或其他用户信息不准确或发生变更的，订户应通知 SZCA 或其授权注册机构，SZCA 或其授权注册机构可配合办理信息更正手续，包括受理信息变更申请，要求补充提供信息变更证明，核实后更正用户注册信息、建议办理证书变更业务。

8.4.3 依法律或行政程序的隐私信息的使用

SZCA 或其授权注册机构仅在司法机关、行政执法机关依法履行职责且按照法定程序要求披露或法律规定必须提供的情况下，会不经订户同意对外提供订户隐私信息。此种情况下的提供隐私信息，是为履行法定义务，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。

在用户同意向司法机关、行政执法机关或监管机构提供、发布其隐私信息的情况下，SZCA 或其注册机构也将配合将私有信息提供给相应授权的人员。

除此以外，SZCA 未取得用户同意不会对外泄露、提供订户隐私信息。

8.4.4 不被视为隐私的信息

发布的订户证书、证书吊销列表（CRL）、证书的状态信息（含吊销、挂起）等，将不被视为隐私信息，是可以公开的。

8.5 知识产权

SZCA 在电子政务电子认证服务中提供的软件、系统、技术接口、网页、文字、图片、文档、数据等各类内容的知识产权归 SZCA 所有，用户在使用 SZCA 服务中所产生的内容的知识产权归用户或相关权利人所有，包括但不限于商标权、专利权、著作权、商业秘密等。

SZCA 在服务中所使用的“SZCA”、企业 logo 及企业形象等商业标识，其著作权或商标权归 SZCA 所有。“深圳 CA”通常情况下指代 SZCA。SZCA 禁止任何个人或单位未经授权商业性使用前述商标、称谓。

上述及其他任何电子政务电子认证服务包含的内容的知识产权均受到法律保护，未经 SZCA、用户或相关权利人书面许可，任何人不得以任何形式进行使用、修改、复制、公开传播、改变、散布、发行或公开发表。

订户、注册机构、依赖方或其他参与方仅拥有相关协议约定合法使用本服务或 SZCA 提供相关技术接口的权利，与本服务相关的技术接口、相关的著作权、专利权等相关全部权利归 SZCA 所有。未经 SZCA 许可，任何人不得违约或违法使用，不得向任何单位或个人出售、转让、授权 SZCA 的代码、技术接口及开发工具等。

8.6 陈述与担保

8.6.1 认证机构的陈述与担保

1.CA 的一般陈述与保证：

- 制定并公布电子认证业务规则（即 CPS）、证书策略（即 CP）等业务必需的业务规则体系。
- 遵守并执行公布的电子认证业务规则（即 CPS）、证书策略（即 CP）。
- 保证证书内容在有效期内完整、准确，并保证电子签名依赖方能够证实或者了解电子签名认证证书所载内容及其他有关事项。
- 保证提供电子签名认证证书信息、证书状态查询服务。

SZCA 及其授权注册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 及其授权注册机构和证书订户的关系、SZCA 及其授权注册机构和依赖方的关系并不是代理人和委托者的关系。

2.CA 对订户、依赖方的陈述与保证：

除非 SZCA 和订户另有约定，SZCA 向证书订户承诺：

- **SZCA 或其注册机构对密钥分发过程中私钥的安全性负责。**
- 除明确标识未经验证的外，证书中的相关信息是准确。
- 在证书中没有 SZCA 或其注册机构已知道或怀疑，应知道或怀疑的源自于 SZCA 或其注册机构的错误陈述。
- 在生成证书时，不会因 SZCA 或其注册机构的失误而导致数据转换错误，即不会因 SZCA 或其注册机构的失误而使证书中的信息与 SZCA 或其注册机构所收到的信息不一致。
- SZCA 按 CPS、CP 的规定撤销或挂起证书。
- SZCA 通过公开发布证书，向所有合理依赖证书信息的人证明：SZCA 已向订户签发了证书，并且订户已接受证书。
- SZCA 将做出合理努力向订户通报任何已知的或可能实质影响签发给订户的证书的有效性和可靠性的重要事件。

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。SZCA 或其注册机构的行为若符合本 CPS 和相关法律的规定，既视为 SZCA 或其注册机构做出了上述描述的合理的努力。

8.6.2 注册机构的陈述与担保

1.注册机构 RA 对订户的陈述与保证

- 遵照法律和 CA 的 CPS、CP 规定，严格认真执行身份鉴别策略，审核证书申请人身份和意愿，审查数字证书业务办理申请。
- SZCA 或其注册机构对密钥分发过程中私钥的安全性负责。

- 除明确标识未经验证的外，证书中的相关信息是准确。
- 在证书中没有 SZCA 或其注册机构已知道或怀疑，应知道或怀疑的源自于 SZCA 或其注册机构的错误陈述。
- 在生成证书时，不会因 SZCA 或其注册机构的失误而导致数据转换错误，即不会因 SZCA 或其注册机构的失误而使证书中的信息与 SZCA 或其注册机构所收到的信息不一致。

2.注册机构 RA 对 CA 的陈述与保证

注册机构 RA 对 CA 机构作出如下陈述与保证：

- RA 保证具备受理用户证书申请的人员、设施、技术条件和服务能力，并能为证书申请者提供证书申请和使用必要的咨询。
- 在 SZCA 授权委托范围内规范开展业务活动，对外以 SZCA 的注册机构或代理机构的名义开展业务。
- RA 必须遵守 SZCA 颁布的网点管理规范、业务受理与服务规范、业务运营管理规范等管理规范，接受 SZCA 对 RA 的业务监督管理，包括但不限于业务操作的合法性、服务质量、服务流程的规范性、业务档案资料保存的完整性等。
- RA 遵守法律政策、SZCA 的 CPS、CP、书面合作协议和其它 SZCA 公布或提供的证书业务流程、要求和标准，受理证书申请者的证书申请，包括告知证书及电子签名的使用条件、法律责任等法定告知事项，审核用户身份和办证意愿，告知用户证书受理结果，要求用户与 SZCA 签署服务协议，向用户安全交付证书。RA 有权决定是否为申请者提供相应的证书服务。但 SZCA 对所有证书申请者的服务请求拥有最终处理权。
- 确保 RA 业务运营系统处在安全的物理环境与网络环境中，并采取必要的技术措施保障 RA 与 CA 之间的数据传输安全，保证依法使用 SZCA 颁发的操作员证书或管理员证书，不得转让或提供他人使用，并保证依法使用 SZCA 的证书相关技术接口及其开发工具、接口文档，未经 SZCA 授权不得提供、转接、转授权给第三方使用。
- RA 必须能够妥善记录保存电子政务电子认证服务相关的信息，包括证书申请人申请、更新、变更、撤销证书等业务时证书申请、审核、受理、通知、签发、接受等全过程业务环节的信息，如证书申请材料、鉴证材料、交付证明资料、证书发放通知等，并按 SZCA 要求向

SZCA 提供 SZCA 指定的证书服务数据资料。重要的是，RA 承诺对用户信息保密等义务，并愿意承担因此而带来的法律责任。

8.6.3 用户的陈述与担保

- 申请证书时，知悉并了解证书对应的 CPS、CP 及订户服务协议的规定，了解证书的使用目的、法律风险和法律后果。
- 保证证书申请中的表述的准确性，包括在证书申请表上填写的信息、提交的资料或陈述的信息是完整、准确、真实、有效的，可供 SZCA 检查和核实；并且，愿意承担任何提供虚假不实等信息的法律责任。
- 一旦接受证书，自接受之时起直至证书有效期满为止，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：

（1） 一旦接受证书，即表示订户同意 SZCA 签发包含其身份信息的证书，同意证书内容中所有信息的真实准确，同意 SZCA 发布证书（除非另行提出异议），且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并未及时通知给 SZCA 或其注册机构，则 SZCA 有正当理由认为：订户认为上述信息都是真实的。

（2） 一经接受证书，既表示订户知悉和接受本 CPS，并知悉和接受相应的订户服务协议。

（3） 妥善保存及安全保护证书私钥及相关密码、口令、密钥令牌等，采取合理措施防止私钥的遗失、泄露、被篡改、损害或被未经授权使用。对于任何实际的或可疑的遗失、泄密或其他对私钥的安全威胁都应立即通报给 CA 或 RA。

（4） 签名时，电子签名人应检查证书确保证书是订户接受的有效证书（证书没有过期、挂起或撤销）。订户接受证书后，除非有相反证据证明，使用证书中所含公钥相对应的私钥所进行的每一次签名，都视为订户的签名。

（5） 在证书用途范围内按照约定的业务目的依法使用证书。

（6） 证书中的所含的订户身份信息（如个人姓名、身份证号，或机构名称、统一社会信用代码，户籍地或住所地）或其他订户信息（如角色、岗位、职位、附属关系）等发生任何改变，应通报给 CA 或 RA。

如果订户委托授权代理人，那么订户和代理人两者负有无限连带

责任：

（a)证书申请者有责任就申请代理人所作的任何不实陈述与遗漏，通知 SZCA 或其注册机构。

（b)订户有责任就授权的第三方电子签名人的签名行为承担法律责任。

需要特别说明的是，除非 SZCA 和订户书面协议明确授权允许，否则订户保证不利用订户证书从事与 SZCA 或其注册机构相同或类似的电子认证业务（含电子政务电子认证业务），例如：把与证书中所含的公钥所对应的私钥用于签发任何终端实体证书（或认证其它任何形式的公钥）或证书撤销列表。

8.6.4 依赖方的陈述与担保

- 依赖方保证在下列情况下方可信赖 SZCA 签发的订户证书或其电子签名：

（1）检查 SZCA 公布的最新的 CRL，确认该证书没有被撤销。

（2）检查该证书信任路径中所有出现过的证书，确认所有证书有效可靠。

（3）检查该证书的有效期以及适用范围，确认证书未过期，证书使用目的是 CPS、CP、服务协议及证书用途扩展项允许的。

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认可和接受 CPS 的规定，尤其是其中有关证书使用、免责、拒绝和限制义务的条款。

8.6.5 其他参与者的陈述与担保

时间戳机构应保证提供的可信时间服务来源于国家权威时间部门（如国家授时中心），并保证时间戳时间的准确性。

8.7 担保免责

对于以下情形，SZCA 将不承担赔偿责任：

（1）由于不可抗力因素导致 SZCA 暂停、终止全部或部分证书服务，SZCA 不承担赔偿责任。

（2）订户违反本 CPS8.6.3 之承诺保证，或者证书依赖方违反本

CPS8.6.4 之承诺保证，导致各自遭受的损失，应由责任方承担，SZCA 不承担任何赔偿、补偿责任；

（3）由于非 SZCA 原因的软件崩溃、硬件故障、网络中断、上游服务中断或错误（如认证数据源中断或数据不准确、国家密钥管理系统升级暂停服务）等导致证书报错、交易中断或其他事由造成的损失，SZCA 不承担责任。

（4）证书订户或者其它有权申请撤销或挂起证书的人提出撤销或挂起请求后，到 SZCA 实际完成证书撤销或挂起期间，如该证书被用以进行非法交易，或者交易产生纠纷的，如果 SZCA 按照本 CPS 的规范进行了有关操作，SZCA 不承担任何损害赔偿责任。

（5）SZC 依据法律法规规定，或应司法机构、行政执法机构、监管部门要求提供电子政务电子认证服务相关材料的，不对此承担法律规定之外的责任。

8.8 偿付责任限制

对于由于 SZCA 违反法律法规、或本 CPS 的原因直接导致当事人损失的，SZCA 将承担相应赔偿责任，用户不能通过合法渠道并提供有效证据证明的除外。

但 SZCA 承担的赔偿责任是有限的。SZCA 只对因使用或信赖证书而产生的直接损失负责，不对间接损害、利润利息损失、精神损害、商誉损失、惩罚性赔偿等承担责任。基于以上赔偿范围，SZCA 及其授权的注册机构，对包括但不限于证书申请者或订户、接受者或依赖方在内的所有当事人的合计赔偿责任，不超过如下所述的对这些证书的赔偿限额。

对于任何人或任何单位有关特定电子签名证书及其交易业务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，包括但不限于包括证书申请者或订户、接受方或依赖方在内的任何人由于使用或信任 SZCA 签发、管理、提供证书发布、证书挂起或撤销等证书状态查询服务的证书（含有效证

书或已过期的证书）而导致的直接损害，及最终确认须承担的补偿性的、间接的、特别的、结果的、惩罚性的或意外的损害。

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，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，且 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，除非相关赔偿得到管辖法院或仲裁机构生效裁决的支持。

8.9 赔偿责任

在签发、管理证书或提供证书服务过程中，因违反法律法规、本 CPS 的规定进行操作，而造成证书订户损失的，SZCA 的赔偿责任承担按照本 CPS“8.8 偿付责任限制”条款执行。

有下列情形之一的，订户应承担由此造成的损失和法律责任：

●订户申请注册证书时，因故意、过失或者恶意提供、陈述不真实不完整不准确的资料或信息，或注册信息发生变化，未及时通知 SZCA、注册机构，或未重新提供新的身份证明资料、信息，导致自身、依赖方、SZCA 或其注册机构遭受损害。

●订户故意或者过失造成其私钥泄漏、遗失、被篡改、遭受损害，明知私钥已经或可能泄漏、遗失、被篡改、遭受损害，如未在安全设备、系统、网络环境中使用，但未及时通知 SZCA 或其注册机构，或未申请证书挂起、撤销，或未停止使用证书，以及不当提供、透露、交付或授权证书给他人使用造成自身、第三方、SZCA 或其注册机构遭受损害的。

●订户使用证书，违反法律法规、CPS 与 CP、服务协议及证书中有关证书使用期限、用途、应用范围等使用规定，如明知证书失效（含证书过期、吊销）仍然使用证书，或将证书用于法律法规及本 CPS 禁止限制的应用或用于违法犯罪或侵犯他人合法权益目的，导致自身、第三方遭受损失。

●订户证书有效期即将届满、证书密码算法、证书密码模块（含证书介质）、证书使用软件程序等不安全、性能不稳定，SZCA 提醒通知进行证书续期、或证书配套软硬件的升级更新但订户未按规定操作，由此造成的使用损失。

●订户未按规定缴纳证书服务费用，SZCA 撤销、注销证书产生的订户、依赖方损失。

●其他订户违反 CPS、CP、服务规范及服务协议规定的相关行为导致的损失。

有下列情形之一的，依赖方应承担由此产生的损失和法律责任：

●依赖方信赖证书时，未依照法律法规、本 CPS、CP、及其他规范及依赖方协议等的规定验证核查证书及其电子签名的可信性，包括对证书未履行合理的注意义务检查证书及其状态，导致自身或第三方遭受损害的；

●依赖方未按规定缴纳应承担的证书服务费用，SZCA 撤销、注销证书产生的订户、依赖方损失；

●依赖方未按照证书应用接口规范集成、接入证书服务，造成的证书签发、使用、验证问题产生的损失；

SZCA 与之签署的协议对赔偿另有规定的，从其规定。

8.10 有效期限与终止

8.10.1 有效期限

本 CPS 自发布后生效，CPS 文件中将详细注明版本号、发布日期、生效日期、失效时间（如有），失效时间如无注明，则为下一新版本 CPS 文件生效的前一日。一般而言，当新版本 CPS 正式发布生效，旧版本 CPS 将自动终止失效。

8.10.2 终止

除本 CPS 另有规定外，本 CPS 在失效后对各方不具有法律约束力。本 CPS 对各当事方的终止失效规则具体为如下：

（1）订户证书因被撤销、注销或有效期届满，或订户注销相关业务平台证书注册、使用信息等各种原因而失效，或订户在法律意义上消亡的，且未再使用 SZCA 任何其他证书的，本 CPS 对订户不再适用；

（2）当依赖方业务平台终止应用 SZCA 数字证书时，CPS 相应地对该特定的依赖方不再适用；

（3）在 SZCA 与外部第三方的注册机构终止合作时，本 CPS 对外部注册机构不再适用；

（4）在 SZCA 终止提供电子政务电子认证服务时，除业务终止的相关业务承接条款外，本 CPS 对 SZCA 不再适用。

本 CPS 失效，不影响 CPS 有效期间各方依照 CPS 开展的行为的法律效力。

8.10.3 效力的终止与保留

本 CPS 中涉及保护保密信息的责任、保护隐私的责任、知识产权、陈述与担保、担保免责、赔付责任限制、争议解决等条款，在本 CPS 终止后仍然继续有效存在。

注册机构在终止业务或其注销时，需将用户证书申请资料、证书认证资料等证书业务过程资料交付转移给 SZCA。

8.11 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，如需与个别订户、依赖方联络沟通或履行通知提醒义务，则须通过 SZCA 或授权注册机构官方客服电话、短信、微信公众号或相关官方平台的站内信、消息等途径，或其他与订户、依赖方书面约定的方式进行。

8.12 修订

8.12.1 修订程序

为保障符合国家法律法规、监管部门政策及国家相关技术标准要求，适应电子政务电子认证业务发展实际需要，SZCA 将不定期对本 CPS 进行审查、评估，并有权根据审查评估结果，进行修订。但 SZCA 将尽量避免对本 CPS 进行不必要的修改。

本 CPS 的修订分为重大修订和非重大修订。重大修订主要指对本 CPS 适用范围、各参与方责任范围、认证流程与规则、CA 认证系统技术安全方面等内容的实质性、重要性修订；非重大修订是指 CPS 因不符合法律法规最新规定，不适应业务发展实际需要而对 CPS 某些方面、某些部分、或个别条款、词句等进行的修订，如个别文字、体例格式、联系方式的改动等。SZCA 对重大修订和非重大修订的区分、认定有酌情权。

具体修订程序详见本 CPS1.4.3“批准程序”。

8.12.2 通知机制和期限

SZCA 有权在认为适当的时间修订和改变 CPS 中任何术语、条件和条款，而且无须预先通知任何一方。

SZCA 通过网站 https://www.szca.com 公布公告修订后的 CPS 文件，不再单独通知订户、依赖方，除非订户、依赖方提出通知推送要求。发布后的 CPS 修订文件将取代在先的相同主题、相同适用范围的原 CPS 文件或其涉及的相关主题的原条款内容。

除通过网站公布 CPS 修订变更文件外，如订户、依赖方需了解 CPS 修订情况或获取 CPS 最新书面文件并提出要求时，SZCA 将按以下规则通知：

●如接受者是公司或其它单位组织，向其申请材料填写的联系地址或工商登记的住所地发送信息。

●如接受者是个人，向其申请材料填写的联系地址发送。

●通知的方式，可采取快递或挂号信、电子邮件、短信、电话或其它方式向订户、依赖方发送通知。

●原则上，对于提供 CPS 书面文本的需求，SZCA 提供 CPS 扫描件、电子件，或提供 CPS 下载获取渠道，不提供纸质 CPS 文件。

8.12.3 必须修改业务规则的情形

如果出现下列任一情况，必须对 CPS 进行修订：

●PKI 技术、密码技术出现重大发展，足以影响现有 CPS 的有效性；

●认证系统和有关管理规范发生重大升级或改变；

●适用的法律法规、监管部门政策、技术标准等规范调整更新；

●现有 CPS 出现重要缺陷；

●应用出现新的要求；

●其他法律法规、技术规范规定 CPS 必须修订的情形。

修订后的 CPS 将在发布后生效，具体生效时间以 CPS 指定的生效时间为准。除非在正式生效前，SZCA 以同样的方式发表一个撤消修订的通知。

8.13 争议处理

本 CPS 相关或由此引发的争议，SZCA 安全策略管理委员会可组织

成立专家组协调处理，专家组负责包括但不限于收集相关的证据，协调SZCA、业务合作方、电子政务电子认证服务注册机构、当事人之间的相互关系，以促进争议解决，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寻求其他法律救济途径。

关于 SZCA CPS 的发布、备案及业务运营行为是否遵照 CPS 执行产生的争议，可向电子政务电子认证服务监管部门国家密码管理局、SZCA 所在地的省级密码管理部门、或其他有关国家部门提起申诉、投诉。

除非争议中的当事人另行书面约定其他争议解决机制（如仲裁）或司法管辖机构，否则就执行 SZCA CPS、SZCA 与任何一方在电子政务电子认证服务中签订的协议，或电子政务电子认证服务活动当事人之间的民商事法律关系有关或由此产生的争议，都应提交到 SZCA 工商注册所在地的人民法院诉讼解决。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处理。

8.14 管辖法律

本 CPS 受《中华人民共和国电子签名法》、《商用密码管理条例》、《电子认证服务密码管理办法》、《电子政务电子认证服务管理办法》以及其它相关适用的中华人民共和国现行法律、法规的管辖和解释。

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，SZCA CPS 的生效、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。

8.15 与适用法律的符合性

SZCA 的电子政务电子认证服务活动及其相关参与方，应遵守《中华人民共和国电子签名法》、《中华人民共和国网络安全法》、《商用密码管理条例》、《电子认证服务密码管理办法》、《电子政务电子认证服务管理办法》。

若本 CPS 所涉及条款，被主管部门或司法机关宣布为非法、不可执行或无效时，或存在明显与最新颁布实施的适用法律法规规定不适应不相符时，该主题相关事项的处理自动适用与原条款本意最接近的现行适

用法律法规规定，同时 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 CPS 某一条款的无效，不影响其余条款的法律效力。

8.16 一般条款

8.16.1 完整协议条款

本 CPS 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。

8.16.2 转让条款

若 SZCA 因不可抗力或其他原因拟暂停或终止提供电子政务电子认证服务，SZCA 对于订户、依赖方的业务及其相关合同权利义务，将按《中华人民共和国电子签名法》《电子政务电子认证服务管理办法》规定转移给其他具有电子政务电子认证服务资质的 CA 机构承接履行，具体以 SZCA 业务通知为准。

除以上原因外，SZCA 对订户及依赖方负有的责任和义务未经订户或依赖方同意，不会以任何形式转让给第三方。

8.16.3 分割性条款

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发现无效或不能执行，那么 CPS 其余的部分不受影响，其他条款规定仍然有效。相关当事人了解并同意，SZCA CPS 所规定的保护保密信息的责任、保护隐私的责任、知识产权、陈述与担保、担保免责、赔付责任限制、争议解决等，均可独立于其它条款，并加以执行适用。

8.16.4 强制执行条款

不涉及

8.16.5 不可抗力条款

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、地震、火灾、疫情、洪水、冰雹、旱灾等；

（2）政府行为，如征收、征用、政府管制等；

（3）社会异常事件，如罢工、骚乱、战争等。

（4）互联网、通讯或其他水电基础设施无法使用。

遭受不可抗力事件影响无法履行合同的，可根据情况全部或部分免除违约责任，但遭受方应在合理时间内尽快通知合同对方和采取合理措施减少对方损失，如停电时启用备份电源。经合同双方协商同意，合同履行时间可合理延长，延长时间相当于因事件发生受到影响的时间。

8.17 其他条款

SZCA 对本 CPS 拥有最终解释权。

附录一

根证名称	证书年限	起止时间	算法
商用SZCA SM2 CA	30年	2019年9月18日-2049年9月10日	SM2
政务SZCA SM2 CA	20年	2013年7月28日-2033年7月23日	SM2
政务RSA2048根证	30年	2018年5月18日-2048年5月10日	RSA2048
粤港互认RSA2048根证	30年	2018年4月25日-2048年4月17日	RSA2048
政务RSA1024根证	20年	2013年4月16日-2033年4月11日	RSA1024