深圳 CA 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：2024年6月7日

深圳 CA 电子认证业务规则

Shenzhen CA Certification Practice Statement

(深圳 CA CPS)

2024年6月7日

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的，受到完全的版权保护。

其它任何个人和团体可准确、完整的转载、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（电子的、机械的、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，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电子认证服务遵从中华人民共和国的法律，对于任何因违反法律行为而影响SZCA电子认证服务的个人、机构或者其它组织，SZCA将保留所有的法律权利，以维护SZCA的利益。

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全文。

2. 本CPS文件规定了SZCA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，已被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及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及其授权证书服务机构。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：518057）。

目录

1 概述性描述

1.1 概述

1.1.1 深圳市电子商务安全证书管理有限公司

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。2006年8月SZCA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》，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，2012年通过卫生部的审核，取得卫生系统电子认证服务资质，并于2016年5月经过工信部核准获得粤港电子签名证书认证资质。上述资质证书目前均处于有效期内。

SZCA依照《中华人民共和国电子签名法》、《电子认证服务管理办法》等法律法规，遵循 PKI 体系标准，向公众（包括政府机构、企事业单位及个人）提供身份认证、数据安全和信任服务，为保证在网络活动中双方身份的真实性、信息的保密性、数据的完整性以及网络活动行为不可抵赖性提供安全服务。深圳CA严格按照工业和信息化部、国家密码管理局等主管部门的要求从事运营服务。

SZCA的根证书体系见附录一。

SZCA与SZCA授权建立的下级CA、注册机构、注册分支机构、服务受理点和其它授权服务代理机构等共同构成SZCA的服务主体体系。

1.1.2 电子认证业务规则

本文件为《SZCA电子认证业务规则》（SZCA Certification Practice Statement，以下简称“本CPS”） 是关于SZCA在数字证书新签发、更新续期、撤销、变更、挂起及密钥更新、密钥恢复等生命周期服务过程中的业务实践所遵循规范的详细描述和声明，是对相关业务、技术和法律责任方面细节的描述。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向社会公布SZCA关于电子认证服务的基本立场和观点，作为实际应用和操作文件的依据，适用于SZCA及其授权机构，订户和依赖方。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，并依此行使权利和承担义务。

1.2 文档名称与标识

1.2.1 文档名称

本文档名称为“SZCA电子认证业务规则”，是关于深圳市电子商务安全证书管理有限公司所提供的电子认证服务相关数字证书签发、管理及服务活动的业务操作规范文件。“深圳CA CPS”、“SZCA CPS”、“深圳CA电子认证业务规则”及其类似表述，无论在任何场所提及，除非另作约定，均应被视为指称本文档或对本文档的引用。

1.2.2 SZCA标识

SZCA所拥有的品牌商标为：  。SZCA的OID包括1.2.156.115215和2.16.156.112548。

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

CA承担证书签发、更新、撤销、密钥管理、证书查询、证书黑名单（又称证书撤销列表或CRL）发布、政策制定等工作。

SZCA和SZCA授权的下级CA统称为电子认证服务机构。SZCA作为被信任的第三方，为电子交易和其它网上作业的参与者颁发数字证书。在SZCA确定参与方的真实身份后，向其发放SZCA数字证书。SZCA数字证书遵循X.509的国际标准。

1.3.2 注册机构

SZCA的注册机构（以下简称“RA”）是经SZCA正式授权的内部或外部业务分支机构，其职能包括面向终端用户受理业务请求，并在SZCA与用户之间互为传递证书服务请求与处理决

定的实体，具体负责受理证书新申请、证书挂起/变更/补办/撤销/更新等服务请求，识别、鉴证证书申请者，处理证书请求，传达通知证书请求受理决定，下载制作证书交付给用户等其中一项或多项工作。

注册机构的业务权限和职责范围由SZCA指定、授权。外部第三方注册机构需与SZCA签署书面合作协议，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。注册机构应承担本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及业务规范开展代理业务。

1.3.3 订户

订户，即证书持有人、最终用户，是指从SZCA接受证书，或实际使用代表其身份的证书并需为使用行为承担法律责任的实体。

订户在申请证书之前建议阅读熟悉CPS、CP相关文件，了解数字证书及其相关产品的用途功能、使用注意事项及其法律后果。订户可以从SZCA及相关网站、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。

证书主体，是指证书面向其签发，其身份与证书绑定关联，其相关身份、标识信息载于证书DN项或证书扩展项的证书主体替换名称，证书用于证明认证其身份、实现数据安全传输等功能的实体。通常情况下，证书发放给为机构、个人等法律主体时，证书主体与订户概念相同，但在证书发放给设备、域名服务器、电子邮箱等无自由意志、无法为自身行为承担责任的非生命实体时，则订户是指发起证书申请、持有控制证书的实体，而证书主体则是指设备、电子邮箱、域名等。

1.3.4 依赖方

在SZCA证书服务体系范围内，依赖SZCA证书进行网上作业的订户，以及依据本CPS合理信任证书真实性的任何实体，称为SZCA的依赖方。依赖方既可以是订户、也可以不是订户。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额外保证，依赖方应在得到这些保证后合理地信任该数字签名。

作为SZCA证书订户的依赖方，享有SZCA提供的各种相应的权利，包括SZCA可能提供的证

书保障，以及本CPS中规定的权益。非证书订户的依赖方，SZCA除了担保其所信任的由SZCA签发的证书和相关签名信息的真实性以外，不承担其他义务和责任。

1.3.5 证书申请者

证书申请者指向SZCA及其授权机构申请证书的实体。任何期望成为SZCA或其下级CA的订户的实体，如符合SZCA规定的证书申请实体条件的，都可以成为SZCA的证书申请者。

证书申请者，应根据其想要获得的证书类型，按照本CPS的规定提供必要的材料、信息，完成申请过程。证书申请者一经提交申请，就意味着已经授权SZCA及其授权的注册机构进行身份鉴别，意味着申请人同意SZCA及其授权机构采用后者认为恰当的方式来确认核实其身份、办证意愿与授权，或所提交的相关材料、信息的真实有效。此处所谓“恰当的方式”与本CPS及相关法律法规要求相一致。

证书申请者，应阅读本CPS及其对应CP、SZCA《电子认证服务协议》，及其他相关服务资料，了解证书业务各方的权利义务。证书申请者在收到证书后，如认为证书内容、质量有问题的，应按规定及时通知SZCA。

证书申请者，应妥善保管证书及其私钥、密码口令，不得以任何方式将其出租、出借、出售、转让给任何其他第三方使用；如发现或应当证书密钥失密或可能失密，或其他有关证书领取接收、使用的异常情况的，应第一时间联系告知SZCA或其授权机构，或向SZCA或其授权机构申请挂起/撤销证书、更新证书密钥。否则，由此造成的损失（如财产损失、可得利益丧失，含不作为造成的扩大部分的损失），证书申请者应承担相应的法律责任。

1.3.6 其它参与者

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数字证书适用于电子政务公共服务、电子商务、医疗卫生、教育、供应链管理、金融、企业信息化、网上信息传递、数据安全等多个领域的应用，详细信息请参阅https://www.szca.com。

1. 证书按证书主体可以分为个人证书、机构证书（含机构个人证书）和设备证书。

2.根据证书的认证方式、存储形态、使用方式等，证书分为硬证书、密钥协同证书。

硬证书，是指证书及其密钥在用户持有控制的硬件密码设备、介质、环境中生成、存储并使用的证书，如USBKEY证书、蓝牙UKEY证书、SIM卡证书、智能卡证书、加密卡或加密机证书等。

密钥协同证书是适用于移动应用、互联网业务场景，通过有效认证措施保障用户控制使用证书密钥，由用户端和服务端共同操作实现签名的证书类型。

前述种类证书包含的以下证书类型，基于其在业务场景应用、证书功能等方面的属性，也对其作以下说明：事件证书、标识证书、时间戳证书。

事件证书是一种基于特定业务场景下的即时、一次性或低频次数据签名/加密等需求签发的数字证书，能保障该业务场景下签署的数据未篡改。SZCA将业务场景中订户提交或订户操作产生的相关业务场景信息（如电子文档哈希值、签名信息、应用方平台信息等）整合写入数字证书中，签发数字证书。该证书仅在该业务场景下的使用有效；脱离该场景的，该证书不能使用，SZCA在此特别声明，不认可其法律效力，也不为此承担责任。

标识证书是指面向应用标识所签发的一种特定证书。这类证书由证书应用平台方提交应用标识， SZCA基于应用平台方提交的证书与应用标识（如应用中的身份账号、身份标识、账号ID、设备标识）绑定对应关系签发证书。证书应用平台方需建立应用标识与对应主体、应用标识与证书的绑定关系，保障标识证书仅可被特定可识别的主体管理与使用。标识证书适用于网络身份、设备或ID的标识、电子签名或数据加密等安全服务，用于证明内部应用标识项下操作的数据不可篡改。

时间戳证书用于明确具体数据创建时间或业务行为在该特定时间节点发生的唯一性，可应用于知识产权保护、电子合同、电子票据、电子档案等领域，这类证书使用数字签名技术并写入从国家授时中心或依靠其他可靠手段获取的标准时间产生签名数据，而签名的对象包

括原始数据、签名参数和签名时间等信息。使用时间戳证书对签名对象进行数字签名所产生的时间戳数据，可以证明原始数据在加盖时间戳时有效存在、唯一性、且内容完整未被篡改。

另外，特别说明的是，测试证书及其签名均不具备法律效力，其是在测试系统、脱产环境中作测试使用，不可应用在正式生产环境中。

1.4.2 限制的证书应用

SZCA签发的证书限制禁止的应用范围包括：

（1）《中华人民共和国电子签名法》规定的禁用情形；

（2）SZCA与订户或依赖方约定的证书限制禁止应用范围；

各类证书的密钥用法及其限制在订户证书的扩展项中予以规定。基于证书扩展项限制的有效性取决于应用软件/应用平台，如果参与方不遵守相关约定，其对证书的应用违反或超出本CPS限定应用范围，将不受SZCA保护或认可。

（3）任何违反国家法律法规强制性规定或危害国家安全的情形。

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。

违反以上证书限制禁止应用范围的规定，造成的损失和法律后果由责任人（含订户）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。

1.5.2 联系人

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：518057】

官网地址：https://www.szca.com

CPS发布地址：https://www.szca.com/service/CPS

1.5.3 决定CPS符合策略的机构

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

1.5.4 电子认证业务规则批准程序

“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、法律法规规定的其他主管部门（如国家密码管理局）备案。

1.6 定义和缩写

表1.1-定义与缩写

缩写/名词	定义
SZCA	深圳市电子商务安全证书管理有限公司的英文名称缩写
电子认证服务机构	电子认证服务机构(Certificate Authority, CA)，SZCA及下级CA统称为电子认证服务机构。
注册机构	简称 RA。SZCA内部设立的负责证书受理发放的部门或机构，或与SZCA签署注册机构合作协议，被SZCA授权发行SZCA证书的代理机构。注册机构负责处理证书申请者提出的证书申请信息，并提交 CA。
发证机构	包含SZCA授权的注册机构、注册分支机构、受理点等证书发放机构。发证机构向证书申请者发放交付SZCA证书。
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	负责实施 CA政策、增加新 CA管理员、验证审计记录、作出电子认证业务规则的执行情况承诺的角色。
SZCA系统管理员	负责安装、配置和维护CA系统的软硬件系统，负责CA服务器的启动和中止。
SZCA录入员	负责录入证书申请者提交的信息。
SZCA审核员	负责审核证书申请信息。
SZCA审计员	CA审计员（Auditor）负责CA系统的证书统计、系统审计等工作。
SZCA证书制作员	负责为证书申请者制作证书。
SZCA数字证书签发系统	为SZCA证书申请者签发、管理数字证书的软件系统。
注册机构协议	一份合同，它详细地概括了SZCA指定的注册机构的业务服务程序、责任和义务。
注册分支机构协议	一份合同，它详细地概括了SZCA指定的注册分支机构的业务服务程序、责任和义务。
依赖方	依赖方（Relying Party）指基于对数字证书或电子签名的信任而从事有关活动的人。

订户	接受、持有、或使用任何SZCA证书的人或实体，包括个人、企业、政府事业单位等
证书申请者	证书申请者（Certificate Applicant）请求SZCA颁发证书的个人、企业或其他组织机构。
参考码	SZCA为证书申请者颁发证书时生成的字符组合，唯一标识证书申请。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，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	唯一标识证书的字符。
甄别名	甄别名（Distinguished Name）简称 DN，包含用户的属性信息。
密钥管理中心	简称 KMC，负责密钥的产生、存储、归档等工作。
OCSP	OCSP（Online Certificate Status Protocol），即在线查询数字证书状态协议，用于支持实时查询数字证书状态。
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。
CRL	CRL（Certificate Revocation List），即数字证书撤销列表的英文简称。CRL中记录所有在原定失效日期到达之前被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。CRL通常又被称为数字证书黑名单。内容通常还包含 CA机构的名称、发行日期、下次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。
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。
私有密钥	指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。 私钥是经由数字运算产生的密钥，用于制作电子签名的数据，亦可依据其运算方式，就相对应的公开密钥加密的文件或信息予以解密。
公开密钥	公钥是经由数字运算产生的密钥，用于解密电子签名，确认电子签名人的身份及电子签名的真实性。 公钥可以公开，一般标示于在线数据库，存储库或其他公共目录中，使任何希望得到公钥的人都能得到。 电子签名验证数据是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。如果电子签名制作数据表现为私钥，则电子签名验证数据就是公钥。

签名密钥对	证书申请者申请证书时由用户端产生。主要用于用户的签名和验证。包含一对私有密钥和公开密钥。
加密密钥对	证书申请者申请证书时由 KMC 产生。主要用于用户信息的加解密。包含一对私有密钥和公开密钥
PKCS	PKCS （Public Key Cryptography Standard），公开密钥密码算法标准

2 信息发布与信息管理

2.1 认证信息的发布

CPS、CP、电子认证服务协议、SZCA业务办理资料及其他相关服务文件、公告通知等可以从SZCA的官网https://www.szca.com 获取;用户证书公开信息可以从SZCA的LDAP上获取;已被撤销的证书信息可以从CRL站点、LDAP查获，而证书的状态（有效、撤销、挂起）可通过OCSP获得。SZCA的官网https://www.szca.com 、LDAP、CRL及OCSP服务器构成SZCA认证信息发布的信息库。SZCA将及时公布更新相关信息。信息库的发布及更改一律须经SZCA核准。除依法必须公开的信息外，具体信息库发布的信息种类与数量因项目情况有所差异。

2.2 发布时间或频率

2.2.1 电子认证业务规则的发布时间及频率

SZCA将及时发布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个工作日内官网https://www.szca.com 上发布。

2.2.2 证书及CRL的发布时间及频率

SZCA完成证书签发后，SZCA将在SZCA信息库上、其指定的其它一个或多个信息库里发布该证书。用户可在SZCA网站https://www.szca.com查询或下载数字证书公开信息。

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;根据需要，也可人工发布最新CRL。CRL在24小时内自动更新，特殊紧急情况下也可通过手动方式变更CRL列表。用户可在SZCA网站https://www.szca.com 上查询或下载最新的CRL。

2.2.3 SZCA公众信息的发布时间及频率

SZCA一旦由于某些原因需要发布与其相关的公告、通知以及其他相关公众信息，SZCA将在官网https://www.szca.com 上进行发布。

2.3 信息库访问控制

SZCA设置了信息访问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官网的在线公告和信息库发布的信息。除非订户、依赖方提出要求，SZCA将发布相关认证信息到信息库。且一般不限制社会公众访问CPS、CP、CRL、公钥证书、服务通知公告文件等信息库信息。但SZCA在认为必要时，在不违反法律法规的情况下，可自主选择并实行信息库的权限管理，或提供有限的认证信息查询获取渠道。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

1. 名称类型

SZCA颁发的证书，含有颁发机构和证书订户主体甄别名，对证书申请者的身份和其它属性进行鉴别，并以不同的标识记录其信息。证书持有者的标识命名，以甄别名（Distinguished Name）形式包含在证书主体内，是证书拥有者的唯一识别名。SZCA的证书符合X.509标准，分配给证书拥有者实体的甄别名。

表3.1-CA颁发机构主体甄别名

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-最终订户证书主体甄别名命名规则

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）；

	● 设备名称或其他唯一标识信息（适用于设备证书）； ● 应用标识（适用于标识证书）； ● 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、标识证书）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】； ● 证书应用平台标识信息（适用于个人证书，标识证书）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具体所在的机构的内部职能部门、下属部门或分支机构所名称； ● 或引用依赖方协议的一个声明，该依赖方协议明确了使用证书的条款； ● 或通告描述证书类型、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）	CN，表示中国
电子邮件（E）	订户的电子邮件地址，或不填

3.1.2 对名称意义化的要求

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

3.1.3 订户的匿名或伪名

除事件证书、标识证书外，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。

3.1.4 理解不同名称形式的规则

关于不同名称的理解，可按照本CPS3.1.1的说明进行。

3.1.5 名称的唯一性

SZCA的所有证书持有者，证书的订户主体项必须是唯一的。如出现重名或同一个订户申请多张数字证书时，各证书通过在证书内容中写入脱敏加密处理后的证件信息、序号、编码（依据一定规则生成）等方式加以区别。

3.1.6 商标的识别、鉴别和角色

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

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

证明拥有私钥的方法是通过PKCS#10的数字签名实现的。SZCA在向订户签发证书前，将使用订户的公钥验证其私钥签名的有效性和申请数据的完整性，以此验证订户拥有私钥。

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，申请者应指定合法授权的证书申请代表，提交经机构盖章或其他方式确认的有效申请材料（包括但不限于身份证明文件、《数字证书申请表》《电子认证服务协议》《个人信息授权书》，具体以SZCA规定的申请材料清单为准），并代表机构签署、确认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》）表示接受证书申请的有关条款，并承担相应的责任。

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：

- 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）；
- 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）；
- 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）；
- 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. 业务办理渠道与要求

组织机构证书申请材料（含身份证明材料）的提交方式，按项目的特性与需求分为以下几种：

（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/授权代表携带本人有效身份证件（参见3.2.3 个人身份鉴别章节个人有效证件有关规定）原件、盖章的含营业执照在内的有效机构证件材料复印件、及其他SZCA要求的申请材料（如《数字证书申请表》《电子认证服务协议》《个人信息授权书》等）盖章原件，亲自到SZCA认可的证书

受理点现场递交证书申请。如以邮寄方式办理的，应按照SZCA要求规范正确完整填写签署相关申请材料后递交证书申请。如SZCA认为有必要的，还可要求核验机构证件原件（有效证件的正本、或副本）。

同时申请机构个人证书的，机构应确保得到各机构个人合法有效的授权，组织机构的经办人/授权代表还应提交盖章的各机构个人有效身份证件复印件，或出具盖章的机构个人办证清单、承诺书等资料（含制作证书所必需的信息）；但出具机构个人办证清单或承诺书等资料的，机构应保证相关个人信息的真实性有效性，且确保各机构个人同意办理证书且愿意向SZCA提交证书制作所需的个人信息。

（2） 线上方式：组织机构经办人/授权代表可通过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、身份证号身份信息）、含营业执照在内的有效机构证件电子影印件（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），及通过在线阅读确认方式签署其他如《电子认证服务协议》《个人信息授权书》有关申请材料、或上传签字盖章的其他如《电子认证服务协议》《个人信息授权书》有关申请材料。并应在SZCA认为必要时，配合SZCA进行人脸识别、机构银行账户小额打款验证码回填等验证工作。

同样，如同时申请机构个人证书，机构应确保得到各机构个人的合法有效授权，经办人/授权代表应提交电子影印件形式的各机构个人有效身份证件，或录入机构个人信息，或上传盖章的机构个人办证清单或承诺书等资料；但出具机构个人办证清单或承诺书等资料的，机构应保证相关个人信息的真实性有效性，且确保各机构个人同意办理证书且愿意向SZCA提交证书制作所需的个人信息。

3. 组织机构身份鉴别流程、方式

对组织机构的身份鉴别，包含组织机构的身份、经办人/授权代表的身份、组织机构中个人的身份，及授权代表授权有效性的核验，具体鉴别验证流程或方式如下：

（1） 检查核对用户申请资料的完整性，包括机构经办人/授权代表是否签署、确认有关《数字证书申请表》《电子认证服务协议》等；

（2） 核对经办人/授权代表身份证件、组织机构证件、机构个人身份证件等所载信息、其他填写提交申请材料相应信息的一致性匹配性；

（3） 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）、红盾网等国家工商数据库、企业征信数据库或其他合法可靠的第三方数据库，或咨询相应的政府机构，或通过组织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、地址等联系组织机构与其确认、实地调查等方式，来验证组织机构是合法真实存在、机构信息真实有效；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） 对于组织机构经办人/授权代表的身份，可通过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）、公安部“互联网+可信身份认证平台”（CTID平台）、公安人口库、驾驶证查询系统等身份信息权威数据源查询，采取活体检测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，验证该经办人/授权代表身份的真实性；机构个人证书，可由机构依赖方提供证书用户名单、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、回填发送至法定代笔人/负责人手机号上的验证码等方式辅助验证，通过组织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、地址等联系组织机构与其确认等SZCA认为合理的方式进行。

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的，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和其授权的证书服务机构将对申请者的材料依法进行审查。

批准申请后，SZCA或其授权注册机构将留存存档申请材料。

SZCA保留根据最新国家政策法规的要求更新机构身份鉴别规范的权利，更新后的机构身份鉴别规范将发布在SZCA的网站。

3.2.3 个人身份的鉴别

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

个人证书包括以下几种证书办理认证模式：

（1）线下方式，包括面对面和邮寄方式，个人可持上述个人有效身份证件原件及复印件，亲自到SZCA授权的注册机构，当场填写签署《数字证书申请表》《电子认证服务协议》等材料，或邮寄个人身份证件复印件及其他SZCA规定的填写签署正确无误的申请材料给SZCA或其授权注册机构。

（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、身份证号身份信息），在线阅读确认方式签署其他如《电子认证服务协议》《个人信息授权书》有关申请材料、或上传签署的其他如《电子认证服务协议》《个人信息授权书》有关申请材料。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。

3. 个人身份鉴别流程、方式

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/设备鉴别证件真伪，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）、公安部“互联网+可信身份认证平台”（CTID平台）、公安人口库、驾驶证查询系统等身份信息权威数据源查询核验，金融银行卡认证、手机号电信验证，面对面审核及人体生物特征识别技术核验，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。

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和其授权的证书服务机构将对申请者的材料依法进行审查。

SZCA授权的注册机构按照SZCA个人身份鉴别规范对申请材料进行审核，并根据鉴别结果进行批准或驳回申请的操作。

批准申请后，SZCA或其授权注册机构将留存存档申请材料。

SZCA保留根据最新国家政策法规的要求更新个人身份鉴别规范的权利，更新后的个人身份鉴别规范将发布在SZCA的网站。

境外国家、地区的机构、个人的身份鉴别，SZCA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。

3.2.4 电子邮箱的鉴别

电子邮箱证书，除参照个人及组织机构身份鉴别要求进行申请人身份鉴别外，还会验证电子邮箱信息。对电子邮箱的鉴别，只会验证电子邮箱是否由用户控制、使用，并不会验证用户是否实名注册此邮箱。对于Email电子邮箱的验证方法：

1. 申请人提交以下申请资料：

- 《数字证书申请表》《电子认证服务协议》等SZCA要求的申请协议材料（具体依用

户申请方式及SZCA服务通知而定）；

- 电子邮件使用人有效身份证件的复印件或电子影印件；
- 如代表机构办理的，经办人/授权代表应提交本人身份证件复印件或影印件，及机构业务授权文件。

2. SZCA向申请人申请的电子邮箱地址发送含验证信息的邮件，用户按邮件验证要求配合进行验证工作，以此核验申请人对邮箱的使用权、控制权。

3.2.5 设备的鉴别

设备证书，除参照个人及组织机构身份鉴别要求进行申请人身份鉴别外，SZCA需要对申请人对设备的所有权、使用控制权进行鉴别。

1. 申请人应提交以下申请材料：

- 《数字证书申请表》《电子认证服务协议》等SZCA提供的申请材料（具体依用户申请方式及SZCA服务通知而定）；
- 申请人有效身份证件的复印件/电子影印件；
- 设备产权证明、使用授权文件或租用借用、购买、转让合同；
- 如代表机构办理证书的，经办人/授权代表还需提交本人身份证件复印件/电子影印件，及机构业务授权文件。

2.SZCA将审核申请材料的完整性真实性，或查询设备产权证明核发机构网站，或联系产权证明颁发机构等方式验证产权证明证件信息。

3.2.6 应用标识的鉴别

应用标识的鉴别，SZCA信任应用平台方建立的应用标识与特定主体的关系，基于此签发标识证书（不含任何实体信息）。

应用平台方提供设备标识信息、平台账号、身份ID（非用户真实姓名）等应用标识，并应保证应用标识与相关实体存在关联绑定关系，该实体知悉并同意向SZCA申请标识证书，并

确保标识证书的使用与管理完全由该实体控制。出现证书办理使用纠纷，应用平台方有责任提供证书使用人身份鉴证资料及使用证明相关材料，并应出面自行与用户解决，承担给用户造成的损失。

3.2.7 没有验证的订户信息

除标识证书、事件证书外，其他未经验证的信息，SZCA不会写入到证书主体项中；如未验证的信息需写入，则会写入到证书扩展项（OA）提示表明该信息未验证。

SZCA对标识证书、事件证书仅提供文件完整性验证、加密密钥恢复等技术服务支持，不提供签名验证、鉴证等取证服务。

3.2.8 授权确认

当自然人或法人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。

3.2.9 互操作准则

SZCA有权依法与合法成立的CA机构等开展有关鉴证服务、数字证书、电子签名的互认互信合作。如与外部机构建立互认关系开展合作，SZCA将按照法律或协议规定开展业务，并将在合作业务中通过包括但不限于官网公告、特定不特定服务对象的服务通知等方式对外公示合作的互认机构信息。

3.3 密钥更新请求的标识与鉴别

SZCA有权根据具体情况决定订户证书有效期长短。在证书有效期届满之前，订户如需续用证书，或如出现证书密钥不安全等情形，应向SZCA或其授权注册机构申请获得新的证书，同时产生一对新的密钥对，称作“密钥更新”。当证书的相关信息发生变化或者对密钥有安全顾虑时，必须重新注册、产生新的密钥对，并向发证机构申请重新签发证书。

3.3.1 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，包括证书更新、证书补办

证书更新，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可依靠原证书申请时提交的信息、及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CPS3.2有关规定。

证书补办，用户按证书新申请流程申请，SZCA按照本CPS3.2进行鉴别。证书补办办理的新证书有效期从新证书签发之日起到原证书有效截止日期/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CPS3.2。

3.3.2 撤销后密钥更新的标识与鉴别

证书撤销后的密钥更新等同于订户重新申请证书，证书撤销后的密钥更新鉴证流程见本CPS3.2。

3.3.3 证书变更的标识与鉴别

证书变更，等同申请新证书，SZCA按照本CPS3.2有关内容进行鉴别，将签发一张新证书，并撤销原证书。

3.4 撤销请求的标识与鉴别

当申请者提出证书撤销申请，且满足本CPS4.9.1所述撤销情形时，注册机构应当审核撤销申请者的书面申请材料和证书DN信息，在审核通过的情况下向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CPS4.9.3第1项。

如果是因订户未履行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，由SZCA、注册机构申请撤销订户的证书，及司法机构等要求撤销证书的，不需要对订户身份进行标识和鉴别。撤销后将SZCA或其授权机构将通知证书订户。

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

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。

4.1.2 注册过程与责任

1. 注册过程

目前，SZCA的证书申请方式有线下申请与在线申请两种方式。申请人使用不同渠道办理证书时，均需首先根据申请证书的类别不同，依照项目情况及SZCA服务指南/通知公告将有关申请资料规范完整填写，并将其他所需资料准备齐全，递交SZCA或SZCA授权注册机构。根据相关法律法规，本CPS规定：申请者必须真实准确规范填写证书申请信息，并遵守SZCA的《电子认证服务协议》及其他有关申请协议，否则SZCA有权拒绝签发证书、停止证书的使用、撤销证书；由此造成的后果，SZCA不承担责任。而后SZCA及其授权机构会依据内部相关流程规定，对申请做出驳回和受理的决定。申请一经受理，则进入审核环节。

2. 各相关当事人的责任

(1) SZCA的责任

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。由于技术的进步与发展，SZCA亦有责任提醒证书订户及时更新证书以保证证书的可靠性。

SZCA应保证其CA机构本身的签名私钥得到安全的存放和保护，其建立和执行的安全机制符合国家相关政策的规定。SZCA亦应保证其整个CA系统安全可靠的运行，由于客观意外或其它不可抗力造成的操作失败或延迟造成的损失、损坏除外。

SZCA应对其授权的证书服务机构进行管理、监督和审计。

(2) 注册机构RA的责任

RA应根据本CPS “3 身份标识与鉴别” 相关规定，在授权范围内收集、审核用户申请资料，鉴别用户身份，并录入用户信息，通过安全通道将用户申请传递给SZCA。

注册机构RA按照规定程序一经取得SZCA的授权，即有义务遵循本CPS、CP与SZCA的书面合作协议、注册机构运营管理规范和其它SZCA公布通知的服务标准和流程文件要求，受理证书申请者的证书服务请求。SZCA将不断完善并及时对其披露有关RA的规范和标准内容。

RA按照SZCA的要求和规范，依据授权设置和管理各类下级证书服务受理机构，包括RA、LRA等，及确定下属证书服务受理机构的设置方式、管理方式和审核方式，这些方式的确定必须以书面的文件形式告知SZCA，涵盖并且不得与SZCA规定的相关条款产生冲突、矛盾或者不一致。

RA依据本CPS的规定，有义务确保其运营系统处在安全的物理环境中，并具备相应的安全管理和隔离措施。RA必须能够提供证书服务全部的数据资料（含证书申请材料、鉴证材料、证书交付证明资料、证书发放通知等）及备份，并按照SZCA的要求，保证其与下属证书服务机构间的信息传输安全。重要的是，RA须严格执行为所有证书用户提供证书业务办理资料（空白模板），妥善保存用户证书办理资料（含用户申请材料、鉴证材料等）及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。

SZCA根据本CPS和授权协议对RA进行管理，包括进行服务资质审核和规范执行检查。SZCA拥有对所有证书申请者服务请求的最终处理权。CA有权对申请者的资料进行复查；因为RA对申请者的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。

(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持有、保管及安全保存的相关程序：

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；并承担一切因填写、提交虚假信息所造成的法律后果。并同意配合SZCA与其授权机构进行相关验证、审核工作，同意授权SZCA与其授权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。

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

证书申请者在申请、接受证书及其相关服务前，需要了解本CPS的条款和与证书相关的证书政策,SZCA在接到证书申请者的任何服务申请时即认为该申请者已经了解本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

订户必须确保将持有的证书用于申请时预定的目的。订户有责任保证私钥的安全。SZCA并不要求证书申请者一定遵从SZCA要求的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，并承担所有因订户的私钥保管出现问题而带来的责任。

一旦发生任何可能导致证书安全性危机的情况，包括订户证书遗失、遗忘私钥或私钥泄密以及其它可能造成订户损失的情况，订户应立刻通知SZCA及其授权的机构，采取申请证书挂起撤销等处理措施。由于通知延误所造成一切损失由证书订户自行承担。

(5) 依赖方的责任

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

依赖方了解本CPS的条款以及和证书相关的证书策略，了解证书的使用目的；

依赖方在信赖SZCA的证书前，有义务查询SZCA公布的最新的CRL，以获得该证书的状态。如CRL显示该证书已撤销作废，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) 目录服务的责任

SZCA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，并在https://www.szca.com公布CRL。

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

4.2 证书审核

4.2.1 证书申请的识别与鉴定

SZCA或授权的发证机构遵循本CPS第3章“3 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，决定申请的批准或驳回。

4.2.2 证书申请的批准与驳回

1. 证书申请的批准

SZCA注册机构成功完成了证书申请所有必须的确认步骤并提交证书请求后，SZCA通过发行正式证书来批准证书申请。证书的签发意味着SZCA最终完全正式地批准了证书申请。如批准申请的，SZCA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授权的注册机构根据其独立判断，有权拒绝签发证书，并且不对因此而导致的任何损失或费用承担任何责任。如果申请者未能成功通过身份鉴别或存在其他不符合申请条件的情形，SZCA将驳回申请者的证书申请。通常情况下，将以适当的方式，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，如无法完成鉴别和验证身份信息；用户没有提交所规定的文件；用户没有在规定时间内回复通知；未收到证书费用等等。被拒绝的证书申请人可再次提出申请。

4.2.3 证书审核时间

在提交的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五个工作日内对证书申请者提交的申请信息进行审核，若延长，需向申请者说明理由。法律或监管政策另有规定的，依其规定执行。

4.3 证书签发

4.3.1 证书签发过程中授权发证机构和电子认证服务机构的行为

SZCA或其授权的注册机构批准证书申请后，用户信息通过安全通道传输发送至SZCA，SZCA签发证书并返回给RA供下载发放。与此同时，SZCA授权的发证机构将证书及证书口令等有关资料（如有）提供给用户。

4.3.2 电子认证服务机构对订户的通告

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

事件证书、标识证书，用户可使用证书、获取证书，即作为SZCA成功签发证书的标志，意味着SZCA已签发证书，SZCA可不再以其他方式另行通知订户。

4.4 证书接受

4.4.1 构成证书接受的行为

在SZCA数字证书签发完成后，SZCA授权的发证机构将会把数字证书及相关资料交给证书申请者。

接受证书的方式包括以下任一方式：受领证书介质、在线成功下载证书、激活证书、获得证书或证书pin码或证书密码或证书口令、使用证书等。

如用户在收到SZCA的证书发放通知，或在应当可以收到证书、使用证书的情况下，无论用户是否实际获得、使用证书，在SZCA或其授权发证机构发放证书（以系统的证书签发记录为准）后24小时内未提出异议的，视为接受证书。

4.4.2 电子认证服务机构对证书的发布

SZCA签发完成的证书将自动发布到LDAP目录服务器中，供订户和依赖方查询和下载。证书订户明确拒绝发布的除外。

4.4.3 电子认证服务机构对其他实体的通告

对于SZCA的证书签发行为，SZCA及其授权注册机构不对其他实体进行通告。

4.5 密钥对与证书的使用

4.5.1 订户私有密钥及证书的使用

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

订户只能在证书密钥用途或服务协议等指定的应用范围内使用私钥和证书，订户只有接受了相关证书之后才能使用对应的私钥，并且在证书到期或被撤销之后，订户必须停止使用该证书对应的私钥。

4.5.2 依赖方证书和公钥的使用

在依赖方接受数字签名信息时需要：

1. 获得数字签名对应的证书和信任链。

2. 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SZCA签发。

3. 检查证书密钥用法扩展项，查看证书的用途适用于对应的签名。

4. 使用证书上的公钥验证签名。

5. 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。

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

4.6 证书更新

4.6.1 证书更新的情形

为保证证书及其密钥对的安全有效，SZCA会为签发的订户证书设置有效期，有效期从签发之日起开始计算。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，方式包括但不限于网站提示、系统提示、书面提示、电话通知、短信通知、电子邮件通知或其它方式，SZCA和其授权的证书服务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。

证书订户如需更新证书，必须在证书有效期届满前一个月内，到SZCA授权的注册机构、发证机构申请作更新证书处理。

4.6.2 请求用户证书更新的实体

参照本CPS4.1.1，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更新。

4.6.3 证书更新请求的处理

证书更新处理流程如下：

SZCA在此提醒：订户在进行证书更新之前，应将原证书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证书的更新。如订户未解密文件而进行证书更新，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/确认签署《数字证书申请表》《电子认证服务协

议》等申请资料，并递交给SZCA授权的注册机构；

- SZCA授权的注册机构对订户提交的证书更新申请进行查验，详情参见本CPS3.2和3.3；
- 注册机构审核通过后，提交申请至SZCA，由SZCA撤销旧证书，签发新证书；
- 注册机构为订户制作证书，将证书及其有关资料发给订户，并通知订户；
- 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。

4.6.4 颁发新证书时对订户的通告

参照本CPS4.3.2

4.6.5 构成接受更新证书的行为

在订户线上、线下方式完成递交更新请求并获得批准后，SZCA或其授权注册机构将按照用户提出更新申请的方式或其他订户、依赖方指定的方式向其发放证书。证书更新接受方式参照本CPS4.4.1。

4.6.6 电子认证服务机构对更新证书的发布

参见本CPS4.4.2

另，新证书签发后，旧的证书将被撤销。SZCA在LDAP目录服务器上发布用户新证书、证书CRL;用户旧证书撤销信息通过CRL发布。

4.6.7 电子认证服务机构对其它实体的通告

参见本CPS4.4.3

4.7 证书密钥更新

当订户或其它参与者需要生成一对新密钥并申请为新公钥签发一个新证书，用户可以选择证书密钥更新服务。出于安全原因，SZCA建议订户证书到期后，选择证书密钥更新，在更

新证书的同时更新密钥。如用户未事先提出需保留使用原证书密钥，证书更新时发证机构默认的方式是为订户同步进行证书密钥更新。

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：

- 证书或其密钥对到期或即将到期(最终订户的私有密钥有效期一般均与其证书的有效期一致）；
- 密钥对已经被泄漏、被窃取、被篡改或者其它原因导致密钥对安全性无法得到保障；
- 证书被撤销后需要重新获得证书；
- 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、服务操作人员等的证书到期前，必须进行证书密钥更新。

证书即将到期的订户，出于安全考虑，应尽量采取证书密钥更新，来获得新的证书。

4.7.2 请求证书密钥更新的实体

参照本CPS4.1.1，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更新。

4.7.3 密钥更新的流程

SZCA在此提醒：订户在进行密钥更新之前，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的更新。如订户未解密文件而进行密钥更新，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/确认签署《数字证书申请表》《电子认证服务协议》有关协议，并向SZCA及其授权机构递交证书密钥更新请求；
- 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CPS3.2和

3.3；

- 注册机构审核通过后，提交申请至SZCA；
- SZCA撤销旧证书，为订户更新密钥、签发新证书；
- 注册机构为订户制作证书，将新证书及其有关资料发给订户，并通知订户；
- 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。

4.7.4 颁发新证书时对订户的通告

参见本CPS4.3.2

4.7.5 构成接受密钥更新证书的行为

参见本CPS4.6.5

4.7.6 电子认证服务机构对密钥更新证书的发布

参见本CPS4.6.6

4.7.7 电子认证服务机构对其他实体的通告

参见本CPS4.4.3

4.8 证书的变更

证书变更是指在订户证书未到期之前，证书内容所含的相关用户信息发生变化，或是证书使用依赖的从属关系发生变化，导致需要变更证书用户信息项相关内容的证书业务类型。订户要变更证书中的内容时，视为申请新证书，证书变更后会导致原证书的撤销。

4.8.1 证书变更的情形

当证书中载明的订户身份或者其它与订户相关的机构从属关系、证书应用依赖方等信息发生变化时，用户必须对原有证书进行变更，向SZCA申请证书变更，SZCA将为用户签发新证

书，同时将撤销原证书。

4.8.2 请求证书变更的实体

参照本CPS4.1.1，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更新。

4.8.3 证书变更请求的处理

SZCA在此提醒：订户在进行证书变更之前，如需使用原证书加密的文件，应在申请证书变更前，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变更申请。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/确认签署《数字证书申请表》《电子认证服务协议》等申请资料，并向SZCA及其授权机构递交证书变更请求，同时应提供原证书有关信息，如证书用户姓名、身份证号、证书DN项、证书序列号，及信息发生变化的证明材料，如最新的身份证件、营业执照、劳动合同解除协议、股东会董事会决议等。

- 注册机构按照本CPS3.2的规定对证书变更申请进行身份鉴别和审核，核实证书所含信息变更情况，注册机构确认并批准变更申请后，向SZCA申请变更证书；

- SZCA撤销旧证书，为订户更新密钥、签发新证书；

- 注册机构为订户制作证书，将新证书及其有关资料发给订户，并通知订户；

- 证书变更完成后，SZCA将证书发布到LDAP目录服务器、证书撤销信息发布到CRL。

新证书的有效期并没有改变，仍然为原证书的剩余有效期/使用期限。证书有效期从新证书签发之日起至原证书有效截止期/失效期止。

4.8.4 颁发新证书时订户的通告

参见本CPS4.3.2

4.8.5 构成接受证书变更的行为

参见本CPS4.6.5

4.8.6 电子认证服务机构对变更证书的发布

参见本CPS4.6.6

4.8.7 电子认证服务机构对其它实体的通告

参见本CPS4.4.3

4.9 证书撤销和挂起

证书撤销是永久性撤销，不可以进行证书恢复。

证书挂起是临时性冻结证书，暂停证书在有效期内的使用；在用户申请等情形下可恢复证书使用。挂起期间，挂起时间计入证书使用时间从证书有效期中扣除，证书有效期不会因证书挂起而中止计算，或因此延长。

4.9.1 证书撤销的情形

1. 新的密钥对替代旧的密钥对；
2. 密钥失密：与证书中的公钥相对应的私有密钥被泄密或用户怀疑私有密钥失密；
3. 从属关系改变：与密钥相关的订户的主体信息改变，证书中的相关信息有所变更；
4. 操作终止：由于证书不再需要用于原来的用途，但密钥并未失密，而要求终止（例如订户离开了某个组织）；
5. 证书服务费用未收到；
6. 订户主体不存在；
7. 订户不能遵守本CPS或其它协议、法律及法规所规定的责任和义务；
8. 订户申请初始注册时，提供不真实材料；

9. 证书已被盗用、冒用、伪造或者篡改；

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

11. 订户申请撤销；

12. 司法机构要求撤销证书；

13. 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；

14. 其它情形。

4.9.2 请求证书撤销的实体

SZCA及其授权机构、证书持有者或其授权人士，有权发起证书撤销申请；特殊情况下，证书持有者所属组织机构或证书使用唯一依赖方，也可申请撤销证书。

4.9.3 证书撤销的流程

1.订户申请撤销流程如下：

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/确认签署《数字证书申请表》《电子认证服务协议》等申请资料，向SZCA及其授权的注册机构递交证书撤销请求，并应注明申请撤销的原因；
- SZCA授权的注册机构遵循本CPS3.2所述对申请者提交的证书撤销申请进行查验，并向SZCA申请证书撤销；
- SZCA验证撤销申请后撤销证书；
- SZCA将证书撤销信息及时发布于信息库供查询；
- 注册机构通知申请者证书撤销。

2.强制撤销

SZCA或其授权的发证机构可以对订户的证书进行强制撤销。强制撤销的命令来自于：SZCA或SZCA授权的发证机构、法院与仲裁机构等司法裁判机构。其他依赖方等怀疑订户证书有安全隐患的，也可向SZCA或其授权的发证机构举报提供线索。

SZCA撤销订户证书后，SZCA或其发证机构将书面或短信等方式通知订户证书被撤销，并通过CRL向外界公布。

4.9.4 撤销请求宽限期

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

4.9.5 电子认证服务机构处理撤销请求的时限

通常情况下，SZCA及其授权证书服务机构在接到客户撤销请求后，48个小时内能够完成证书撤销流程，并在CRL上公布。法律法规另有规定的，依其规定执行。

4.9.6 依赖方CRL 检查要求

依赖方应经常检查CRL，包括：

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

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

4.9.7 CRL 发布频率

SZCA证书撤销列表在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。

4.9.8 CRL发布最大滞后时间

CRL 发布的最大滞后时间为24 小时。

4.9.9 OCSP的可用性

SZCA提供证书状态的在线查询服务，该服务7X24小时可获得。

4.9.10 OCSP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。

4.9.11 撤销信息的其他发布形式

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。

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撤销证书。

4.9.13 证书挂起情形

证书挂起，在SZCA业务类型中，又称为证书“冻结”。

证书用户因自身原因，如长期出差，短期内无法使用证书，或证书有丢失、泄密风险需先紧急申请挂起暂停使用证书，可以申请证书挂起。SZCA或SZCA授权的发证机构也有权在认为必要时，执行强制挂起，强制挂起后必须立即通知该订户。

4.9.14 请求证书挂起的实体

参照本CPS4.9.2

4.9.15 证书挂起的流程

1．订户申请证书挂起

- 申请者提交身份证件、填写签署/确认签署《数字证书申请表》《电子认证服务协议》等申请资料，或通过在线客服电话、远程视频等方式，向SZCA及其授权注册机构递交证书挂起请求，并应注明申请挂起的原因、挂起时间，业务类型选择“冻结”；

- SZCA授权的注册机构遵循本CPS3.2规定对订户提交的证书挂起申请进行查验，并向SZCA申请证书挂起，由SZCA执行证书挂起；

- SZCA将挂起的证书发布到CRL；

- SZCA挂起订户证书后，注册机构通知订户证书已被挂起。

2.强制挂起证书

SZCA有充分合理理由的可以依法对订户证书进行强制挂起，并将挂起原因及其相关依据记录在册，挂起后必须通知该订户。强制挂起的命令来源于：SZCA或SZCA授权的发证机构、法院与仲裁机构等司法裁判机构。

订户证书的挂起申请处理时间最长不超过48个小时。

4.9.16 挂起的期限限制

订户证书的挂起时间最长不超过3个自然日，到期后订户未及时申请证书撤销的，SZCA将恢复证书。对此造成的任何后果， SZCA不承担任何责任。

4.9.17 挂起证书的恢复流程

挂起证书恢复的具体流程如下：

- 申请者提交身份证件、填写签署/确认签署《数字证书申请表》《电子认证服务协议》等，或通过电话、远程视频等能够有效核实申请人身份和办理意愿的方式，向SZCA及其授权注册机构递交证书挂起请求，并应注明申请挂起的原因，业务类型选择 “解冻”项；

- SZCA授权注册证机构遵循本CPS3.2所述对订户提交的证书恢复申请进行查验；
- 注册机构审核通过后，向SZCA申请恢复证书；
- SZCA将挂起证书移出CRL，为订户恢复证书；
- 注册机构通知订户证书已被恢复。

4.10 证书状态查询

4.10.1 操作特征

SZCA提供两种状态查询服务：

1.CRL

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

2.OCSP

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

4.10.2 服务可用性

SZCA提供7X24小时的证书状态查询服务。

4.11 服务终止

服务终止是指订户终止与SZCA的服务，它包含以下两种情况：

- 证书到期时终止与SZCA的服务；

当证书到期时，订户不再延长证书使用期或者不再重新申请证书时，视为服务终止。

- 证书未到期时终止与SZCA的服务。

在证书的有效期内，由于订户的原因而单方面要求终止证书服务，SZCA将根据证书使用者的要求撤销证书；如因其他客观原因导致订户无法继续使用证书的，SZCA也可撤销证书。在撤销证书时如用户未新申请证书，订户与SZCA的服务在证书撤销完成后终止。

4.12 密钥生成、备份与恢复

4.12.1 签名密钥的生成、备份与恢复的策略与行为

通常订户签名密钥对由订户的密码设备或经国家密码管理局认可的商用密码产品（密码模块）生成，由用户自行保管。

协同签名证书，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。

SZCA在此提醒订户务必妥善保管证书私钥。由于签名私有密钥遗失所造成的损失由订户自己承担，SZCA概不负责。

加密密钥对由密钥管理中心生成，密钥管理中心只能恢复订户的加密密钥，故SZCA仅提供订户证书加密密钥恢复服务，不支持签名密钥恢复。

4.12.2 加密密钥的生成、备份和恢复的策略和行为

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

1. 由于加密密钥丢失或其他原因，订户需要进行证书恢复的情形

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

2. 国家执法机关、司法机构因执法、司法或国家其它管理部门管理或取证的需要

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

3. 密钥管理中心认为有必要。

5 认证机构设施、管理与操作控制

5.1 物理控制

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

5.1.1 场地位置与建筑

SZCA认证系统的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。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。

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。

5.1.3 电力与空调

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

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

5.1.4 水患防治

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

5.1.5 火灾防护

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

5.1.6 介质存储

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

5.1.7 报废处理

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

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

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

5.1.8 异地备份

SZCA对重要数据进行异地备份，遇到灾难情况发生时保证数据安全。

5.2 程序控制

5.2.1 可信角色

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

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

- SZCA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。

5.2.2 每项任务需要的人数

表5.1-可信角色最低人数配备

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

5.2.3 每个角色的识别与鉴别

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

所有SZCA关键职位人员必须确保：

1. 发放的安全令牌只直接属于个人或组织所有；

2. 发放的安全令牌不允许共享；

3. SZCA的系统和程序通过识别不同的令牌，对操作者进行权限控制。

5.2.4 需要职责分割的角色

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

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

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

5.3 人员控制

5.3.1 资格、经历和无过失要求

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

SZCA对承担可信角色的工作人员应具备的基本条件如下：

1. 具备良好的社会和工作背景；
2. 遵守国家法律、法规，服从SZCA的统一安排及管理；
3. 遵守SZCA有关安全管理的规范、规定和制度；
4. 具有良好的个人素质、修养以及认真负责的工作态度；
5. 具备良好的团队合作精神。

5.3.2 背景审查程序

SZCA员工的录用须经过严格的可信背景调查，且需要有不少于3个月的试用期，未通过初次背景调查的员工，一律不得录用。可信人员背景调查及信誉度调查定期进行，原则上3年一次，SZCA根据实际情况可增加调查次数。

背景调查分为基本调查和高级调查。

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

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

调查程序包括：

(1) 人事部门负责对应聘人员的个人资料予以确认。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。

5.3.3 培训要求

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

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

5.3.4 再培训周期和要求

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

5.3.5 工作岗位轮换周期和顺序

SZCA根据自身需要安排工作轮换，轮换周期视具体情况而定。

5.3.6 未授权行为的处罚

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

5.3.7 独立合约人的要求

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

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

5.3.8 提供给员工的文档

在培训或再培训期间，SZCA提供给员工的培训文档包括但不限于以下几类：

(1) SZCA员工手册；

(2) SZCA电子认证业务规则；

(3) SZCA技术体系文档；

(4) SZCA安全管理制度等。

5.4 审计日志程序

5.4.1 记录事件的类型

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

(1) CA密钥生命周期内的管理事件，包括密钥生成、备份、恢复、归档和销毁；

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

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

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

(5) 系统巡检记录；

(6) 人员访问控制记录。

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

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

5.4.2 处理日志的周期

SZCA每月对记录进行审查，对审查记录行为备案。

5.4.3 审计日志的保存期限

SZCA审计日志在线记录至少保存1个月，离线存档至少7年。

5.4.4 审计日志的保护

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

5.4.5 审计日志备份程序

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

5.4.6 审计收集系统

应用程序、网络和操作系统等都会自动生成审计数据和记录信息，并进行归类。

5.4.7 对导致事件实体的通告

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

5.4.8 脆弱性评估

在认证系统运行时，SZCA从内部和外部包括系统资产、系统安全措施运行情况等方面对系统可能遭受的威胁进行评估，并根据日志的日常审计和管理措施的监督实施，随时调整和系统运行密切相关的安全控制措施，以便将系统运作的风险降到最低。

5.5 记录归档

5.5.1 归档记录的类型

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

5.5.2 归档记录的保存期限

SZCA的订户证书及其申请资料存档期限为：证书失效后5年。法律规范另有规定的依其规定，如电子政务用户的证书相关资料保存至证书失效后10年。

5.5.3 归档文件的保护

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

5.5.4 归档文件的备份程序

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

5.5.5 记录时间戳要求

所有 5.5.1 条款所述的存档内容都加时间标识。

5.5.6 归档收集系统

SZCA档案的收集系统由人工操作和自动操作两部分组成。

5.5.7 获得和检验归档信息的程序

SZCA定期验证存档信息的完整性。

5.6 电子认证服务机构密钥更替

当CA根密钥对累计寿命超过本CPS6.3.2中规定的最大有效期时，SZCA将启动密钥更新流程。旧的CA密钥对到期前，SZCA将用新的CA密钥对签发证书。

5.7 损害与灾难恢复

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

5.7.1 事故和损害处理程序

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

5.7.2 计算资源、软件或数据的损坏

当认证系统运营使用的软件、数据或者其它信息出现异常损毁时，可以依照SZCA灾难恢复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。

5.7.3 实体私钥损害处理程序

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

5.7.4 灾难后的业务连续性能力

SZCA在遭遇本CPS5.7.1和5.7.2中描述的灾难后，将启动SZCA灾难恢复计划，在最短的时间内恢复各项业务的正常运行。

5.8 电子认证服务机构或注册机构的终止

当SZCA及其授权服务机构需要终止经营时，将会按照《电子认证服务管理办法》等法律法规之规定执行。

6 认证系统技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

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的、SZCA数字证书签发系统支持的介质、或商用密码产品（密码模块）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。

选择事件证书的，密钥对由负责业务应用的平台应用方承担保管责任，保障密钥对的存储安全，及通过安全认证、控制措施确保由用户使用的使用安全。

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。

6.1.2 私钥传送给订户

通常，订户证书的签名密钥对由用户自己生成并保管。用户如委托SZCA产生密钥时，SZCA将以离线方式安全传送，确保私钥在交付用户前未被使用。

事件证书，订户密钥对由负责业务应用的平台应用方保管，密钥对通过安全认证、控制措施保障由订户控制。

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。

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。

6.1.3 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道，经注册机构传递到SZCA。

订户的加密证书公钥由KMC通过安全通道传递到CA中心。

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

6.1.4 电子认证服务机构公钥传送给依赖方

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

6.1.5 密钥的长度

SZCA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不建议订户使用RSA 1024位密钥对的数字证书，也不推荐签发1024位的RSA算法的数字证书。

6.1.6 公钥参数的生成和质量检查

公钥参数由国家密码管理局许可、SZCA数字证书签发系统支持的硬件产生。

6.1.7 密钥使用目的

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

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。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块的标准和控制

SZCA的CA系统使用通过国家密码主管部门鉴定并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。

6.2.2 私钥多人控制

SZCA从技术和制度上保证了敏感的加密操作需要在多个可信角色的共同参与下才能完成。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。

6.2.3 私钥托管

对于CA根证书密钥SZCA无托管业务；对于订户加密证书私钥的托管，由国家规定的密码管理机构进行。订户签名密钥的托管（如有）SZCA按照国家法律法规执行。

6.2.4 私钥备份

- CA的私钥保存在防高温、防潮湿及防磁场影响的环境中，对私钥的备份操作必须2人或以上才可完成。
- SZCA对CA的私钥有多机备份，在有私钥变动时做数据备份。

6.2.5 私钥归档

当SZCA的CA密钥对到期后，这些密钥对通常将被归档保存至少5年，法律法规另有规定除外，如面向政务部门服务的CA密钥对的保存归档期限应按法律法规规定保存至少10年。归档的CA密钥对保存在本CPS6.2.1所述的硬件密模块中，当其保存期满时，SZCA将按照本CPS6.2.10所述方法进行安全地销毁。

订户加密密钥的归档由KMC负责。SZCA不对RA和订户签名密钥归档。

6.2.6 私钥导入、导出密码模块

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

订户通过密码设备生成的签名私钥不可导出密码模块。

6.2.7 私钥在密码模块的存储

订户私钥在硬件密码设备或密码模块中加密保存。

6.2.8 激活私钥的方法

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

6.2.9 解除私钥激活状态的方法

具有解除私钥激活状态权限的管理员使用含有自己身份的加密IC卡登录，启动密钥管理程序，并进行解除私钥的操作，需要3名管理员同时在场监督。

6.2.10 销毁私钥的方法

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

6.2.11 密码模块的评估

由国家密码管理部门负责。

6.3 密钥对管理的其它方面

6.3.1 公钥归档

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

6.3.2 证书操作期和密钥对使用期限

订户证书有效期通常不得超过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。

6.4 激活数据

6.4.1 激活数据的产生和安装

CA私钥的激活数据，必须按照关于密钥激活数据分割和密钥管理办法的要求，严格进行

生成、分发和使用。

订户的激活数据包括下载证书的口令、用户密钥存储介质的PIN码等。下载证书的口令由SZCA在安全可靠的环境下随机产生，通过可靠的方式发送给订户。证书存储介质（如：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。为保证私钥安全，SZCA推荐订户使用密码口令。

6.4.2 激活数据的保护

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

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

6.4.3 激活数据的其它方面

考虑到安全因素，对于订户激活数据的生命周期，规定如下：

1. 订户用于下载证书的口令，下载成功后失效。

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

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

SZCA的数字证书签发系统的数据文件和设备由SZCA系统管理员维护，未经SZCA管理员授权，其它人员不能操作和控制SZCA系统；其它普通用户无系统账号和密码。SZCA系统部署在多级不同厂家的防火墙之内，确保系统网络安全。

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

6.5.2 计算机安全评估

SZCA使用的密码设备是通过国家密码管理局批准生产的密码设备。计算机的安全检测评估将由内部专业人员或委托外部具备专业资质的机构进行。

6.6 生命周期技术控制

6.6.1 系统开发控制

SZCA的系统由具有商用密码产品研发资质的可靠开发商按照国家相关的安全标准开发，其开发过程符合SZCA系统管理的各项规定。

6.6.2 安全管理控制

SZCA的配置以及任何修改和升级都会记录在案并进行控制，并且SZCA采取一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。

6.6.3 生命期的安全控制

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

6.7 网络的安全控制

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

7 证书、证书撤销列表和在线证书状态协议

7.1 证书

SZCA使用详细证书格式符合国家相关标准要求，是ITU-T推荐的国际标准。

7.1.1 版本号

SZCA签发的证书符合X.509 V3 版证书格式。

7.1.2 证书标准项

- 证书版本号(Version) ：指明X.509证书的格式版本，值为V3。
- 证书序列号（Serial Number）：即由SZCA分配给证书的唯一的数字型标识符。
- 签名算法标识符（Signature）：指定由SZCA签发证书时所使用的签名算法。
- 签发机构名（Issuer）：用来标识签发证书的CA的X.500 DN名字。

CN = SZCA

OU = SZCA

O = Shenzhen Certificate Authority

L = Shenzhen

S = Guangdong

C = CN

- 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。
- 证书主体（Subject）：指定证书持有者的X.500唯一名字。包括国家、省、市、

组织机构、单位部门和通用名，还可包含E-mail地址等个人信息等。

- 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。
- 微缩图算法：SZCA对证书内容的签名算法。
- 微缩图：SZCA对证书内容的签名值。

7.1.3 证书扩展项

1、证书标准扩展项

- 颁发机构密钥标识符（Issuer Unique Identifier）：此域用在当同一个X.500名字用于多个认证机构或同一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。
- 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：指定各种密钥的用法：电子签名，不可抵赖，密钥加密，数据加密，密钥协议，验证证书签名，验证CRL签名，只加密，只解密，只签名。
- CRL发布点：由SZCA定义的CRL发布点。
- 其他RFC5280规定的证书扩展项。

2、自定义扩展项

针对不同的证书应用服务SZCA自定义了包括但不限于以下扩展项：

- 企业标识：指定企业的唯一标识符。
- 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。
- 组织机构代码：此域用来记录机构的组织机构代码。

- 注册号：指定机构、企业的注册号。
- 统一社会信用代码：指定组织机构的统一社会信用代码。
- 登记机关：指定机构、企业的登记机关。
- 法人(负责人)：指定机构、企业的法人(负责人)名称。
- 身份证号：指定机构、企业的法人/负责人，或个人的身份证号。
- 岗位名称：指定机构、企业内工作岗位的名称。
- 机构签名证书序列号：指定机构、企业证书中签名证书序列号。
- 业务/场景属性：指定证书所适用的业务属性。
- 项目类型：指明证书所应用的项目类型、或行业应用类型
- 扩展代码：可用于指定机构/企业业务证书颁发的数量。
- 扩展标识：指定项目应用标识所需信息。
- 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。
- 岗位责任人：指定机构/企业业务证书中所在岗位的责任人。
- 岗位责任人身份证号：指定机构/企业业务证书中所在岗位的责任人身份证号。

7.1.4 算法对象标识符

SZCA签发的证书中，采用SHA1withRSA、SHA256withRSA、SM3withSM2三类组合密码算法，其对应密码算法的标识符为1.2.156.197.1.505、1.2.156.197.1.506、1.2.156.10197.1.501。

7.1.5 名称形式

SZCA签发的证书名称形式的格式和内容符合X.500 Distinguished Name(DN)的甄别名格式。详见本CPS3.1。

7.1.6 名称限制

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

7.2 CRL（证书撤销列表）

SZCA定期签发 CRL（证书撤销列表），供用户查询使用。SZCA签发的 CRL 遵循 RFC3280 标准。

7.2.1 CRL版本

SZCA的证书撤销列表采用X.509 v2 版的证书格式。

7.2.2 CRL项和CRL条目扩展项

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

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

  L=SHENZHEN

  S=GUANGDONG

  C=CN

- 生效时间：此次CRL的生效时间。
- 下一次的更新时间：下次CRL签发时间。
- 签名算法：SZCA采用SHA1withRSA、SHA256withRSA、SM3withSM2签名算法。
- 颁发机构密钥标识符（Issuer Unique Identifier）：此域用在当同一个X.500名字用于多个认证机构时，用来唯一标识签发者的X.500名字。
- 撤销证书列表：每个证书对应一个唯一的标示符(即它含有已撤销证书的唯一序列号，并不是实际的证书，废除的证书序列号是指要废除的由同一个CA签发的证书的一个唯一标识号，同一机构签发的证书不会有相同的序列号)。列表中的每一项都含有

证书不再有效的时间。

- CRL发布：SZCA周期性自动发布最新的CRL。

7.2.3 CRL下载

SZCA证书用户可以通过SZCA网站https://www.szca.com下载CRL。

7.3 OCSP（在线证书状态查询服务）

SZCA通过OCSP为用户提供证书状态实时查询服务。

7.3.1 OCSP版本号

SZCA在线证书状态协议为v1版。

7.3.2 OCSP扩展项

SZCA的OCSP不支持使用扩展项。

8 认证机构审计与评估

8.1 评估的频率与情形

SZCA在如下情形中进行评估：

(1) 内部评估：SZCA安全策略管理委员会定期不定期按照规定的评估方法和过程，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。

(2) 外部评估：根据《中华人民共和国电子签名法》《中华人民共和国密码法》《电子认证服务管理办法》《电子认证服务密码管理办法》等规定接受主管部门的评估和检查，频率由主管部门根据相关法律法规决定。电子认证密码服务管理办法。

8.2 评估者的资质

SZCA的内部评审由SZCA安全策略管理委员会负责，其成员为具有多年行业经验的高级管理人员及核心技术人员。

如果SZCA认为有必要聘请外部的审计者实施内部审计，那么对SZCA实施规范审计的审计者所具有的资质和经验必须符合监管法律和行业准则规定的要求，包括：

- 必须是经许可的、有营业执照的、具有计算机安全专门技术知识的审计人员或审计评估机构，且在业界享有良好的声誉。
- 了解计算机信息安全体系、通信网络安全要求、PKI 技术标准和操作。
- 具备检查系统运行性能的专业技术和工具。

8.3 评估者与被评估者之间的关系

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，也应是独立的关系，没有任何的利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对被评估的对象进行评估。

8.4 评估内容

对SZCA评估内容包括但不限于：

- 人事审查；
- 物理环境建设及安全运营管理规范审查；
- 系统结构及其运营审查；
- 密钥管理审查；
- 客户服务及证书处理流程审查。

8.5 对问题与不足采取的措施

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

SZCA完成内部评估后，评估人员需要列出所有问题项目的详细清单，由评估人员和被评估对象共同讨论有关问题，并将结果书面通知SZCA安全策略管理委员会和被评估者，进行后续处理。

SZCA将根据普遍认可的国际惯例或监管法律迅速解决问题。

8.6 评估结果的传达与发布

SZCA只按管理或协议要求将审计或评估结果传达到相应对象，除非法律法规要求，SZCA将不公开审计或评估结果。SZCA内部评估结果处分权归SZCA所有。任何人未经SZCA许可发布或泄漏的审计或评估结果，SZCA将保留追究其法律责任的权利。

9 法律责任和其它业务条款

9.1 费用

证书相关费用在SZCA的网站https://www.szca.com上公布。价目表按SZCA明确指定的时间生效，若没有指定生效时间的，自价目表公布之日起生效。SZCA也可以通过其它方法通知订户或其它各方费用变化。

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

9.1.1 证书签发和更新费用

参见CPS9.1。

9.1.2 证书查询费用

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

9.1.3 证书撤销或状态信息的查询费用

对于SZCA公开的证书撤销或状态信息的查询，SZCA不收取查询费用；但是对于客户提出的高时效性或其他特殊证书状态查询服务项目，SZCA保留收取费用的权利。

9.1.4 其它服务费用

参照CPS9.1，具体依客户需求、服务性质等项目情况为定。

9.1.5 退款策略

在实施证书操作和签发证书的过程中，SZCA遵守并保持严格的操作程序和退款策略。一旦发放数字证书，SZCA将不办理退证退款手续。除非订户可以通过合法途径证明SZCA违背了

CPS 有关订户或订户证书方面所规定的责任或其它重大义务，否则SZCA向用户收取的费用均不退还。因为证书撤销等原因确实需要退还预付费用的，订户需要填写退款申请表，并发送给SZCA，以要求退款。此退款策略不限制订户得到其它的赔偿。完成退款后，订户如果继续使用证书，SZCA将追究其法律责任。

9.2 财务责任

9.2.1 保险范围

SZCA根据业务发展情况决定其投保策略。

9.2.2 对最终实体的保险和担保

根据《中华人民共和国电子签名法》的规定，订户在此同意：由于SZCA的责任给订户造成的直接损失，SZCA仅赔偿订户一定金额的直接损失，即SZCA将根据使用证书的种类，承诺一定额度的赔付具体情况参见本CPS9.8。

9.3 业务信息的保密

9.3.1 保密信息范围

保密信息包括但不限于以下内容：

1. SZCA与SZCA授权的注册机构之间、SZCA与订户之间、SZCA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. 与证书持有者证书公钥配对的私钥；
3. SZCA或SZCA对注册机构的审计记录、审计报告、审计结果等；
4. 有关SZCA认证体系的运营信息；
5. 灾备计划、应急方案、安全措施等内部流程管制文件；
6. 订户证书信息以外的个人隐私信息。

以上信息除非法律明文规定或政府、执法部门等的要求，或SZCA认为有必要，SZCA没有义务也不会对外公布或披露。

9.3.2 非保密信息

1.与证书有关的申请流程、申请需要的手续、申请操作指南、CPS等；

2.证书持有者证书中包括的相关公开信息；

3.证书状态及撤销列表信息；

4.其他可以通过公共、公开渠道获得的信息；

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

其它SZCA信息的保密性取决于特殊的数据项和申请。

9.3.3 保护保密信息的责任

SZCA、任何订户、关联体以及与认证业务相关的参与方等，皆有义务按照本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、法规或规章条款的要求下，或在法院的要求下披露本CPS所载具有保密性质的信息时，SZCA可以按照法律、法规条款以及法院、仲裁机构等裁判的要求，向执法部门披露相关的保密信息。这种披露视为不违反保密的要求和义务。

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

9.4 个人信息的保密

9.4.1 隐私保密方案

SZCA的隐私保密政策与方案，按照我国信息安全方面的法律法规的要求和国际公认的个人数据隐私保护原则执行，本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，那么就表示已经同意接受SZCA有关隐私保护的声明（如《个人信息保护政策》）。

9.4.2 作为隐私处理的信息

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

9.4.3 非保密的个人信息

证书订户持有的证书内包括的信息，以及该证书的状态信息等，是可以公开的，将不被视为隐私信息。如属于用户所有且订户要求仅在特定范围内公开的个人信息，SZCA应响应订户要求。

9.4.4 保护隐私的责任

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

当SZCA在任何法律法规规定，或公安机关、法院等行政执法、司法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，SZCA可以向特定对象披露相关的隐私信息。SZCA无须为此承担任何责任，而且这种披露不被视为违反了隐私保护义务。如果这种隐私披露导致了任何损失，SZCA对此不应承担任何责任。

9.4.5 使用隐私信息的告知与同意

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

SZCA在任何法律法规规定或者法院等行政执法机关、司法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客户隐私信息用于双方约定的用途以外的目的，在法律允许的情况下，事前需告知订户，并得到用户的同意和书面授权。

9.4.6 依法律或行政程序的信息披露

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

- 政府法律法规的规定并且经过主管单位合法的授权程序提出申请；
- 法院、仲裁机构等司法裁判机构处理因使用证书产生的纠纷或仲裁时合法的提出申请；
- 国家司法机关、行政执法机关开具证明需我司配合取证，例：公安、检察院、法院、工商局等；
- 证书订户以书面方式进行授权。

9.4.7 其它信息披露情形

其它信息披露亦需在法律法规和订户协议许可范围内。

9.5 知识产权

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

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

在没有SZCA事先书面同意的情况下，任何使用者不能在任何证书到期、作废或终止后，使用或接受任何SZCA使用的名称、商标、交易形式或可能与之相混淆的名称、商标、交易形式或商务称号。

9.6 陈述与担保

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

9.6.1 电子认证服务机构的陈述与担保

1. SZCA的一般陈述与保证：

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

2. SZCA对订户的陈述与保证:

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

- 在证书中没有发证机构所知的或源自于发证机构的错误陈述。

- 在生成证书时，不会因发证机构的失误而导致数据转换错误，即不会因发证机构的失误而使证书中的信息与发证机构所收到的信息不一致。

- 发证机构签发给订户的证书符合本CPS 的所有实质性要求。

- 发证机构将按本CPS的规定，及时撤销或挂起证书。

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

- 发证机构将做出合理努力向订户通报任何已知的，将在本质上影响签发给订户的证书的有效性和可靠性的事件。

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

3. 发证机构对依赖方的陈述与保证：

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

- 除了未经验证的订户信息外，证书中的或证书中合并参考到的所有信息都是准确的。

- 发证机构完全遵照本CPS 的规定签发证书。

9.6.2 注册机构的陈述与担保

注册机构RA按照程序取得了SZCA的授权后，将保证：

- 遵循本CPS和SZCA的授权协议和其它SZCA公布的标准和流程，接受并处理证书服务申请者的证书服务请求。

- RA必须遵循SZCA制订的服务受理规范、系统运作规范和管理规范，根据本CPS、SZCA公布的规范，RA有权决定是否为申请者提供相应的证书服务。

- 按照SZCA的要求和规范，依据授权设置和管理各类下级证书服务受理机构，包

括RA、LRA等，并确定下属证书服务受理机构的设置方式、管理方式和审核方式，这些方式的确定必须以书面的文件形式存档，涵盖并且不得与SZCA公布的相关条款产生冲突、矛盾或者不一致。

- 依据本CPS的规定，确保其运营系统处在安全的物理环境中，并具备相应的安全管理和隔离措施。RA必须能够妥善保存并按SZCA要求向SZCA提供证书服务全部的数据资料（含证书申请材料、鉴证材料、交付证明资料、证书发放通知等）及备份，并按照SZCA的要求，保证其与下属证书服务机构间的信息传输安全。重要的是，RA承诺严格执行为所有证书用户提供证书业务办理资料（空白模板），妥善保存用户证书办理资料（含用户申请材料、鉴证材料等）及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。

- 接受SZCA根据本CPS和授权协议对RA进行管理，包括进行服务资质审核和规范执行检查。

- 承认SZCA对所有证书申请者的服务请求拥有最终处理权。

- 为证书申请者提供必要的技术咨询，使证书申请者顺利地申请和使用证书。

9.6.3 订户的陈述与担保

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

- 在证书申请表上填列的声明和信息或其他提交的资料、陈述的信息必须是完整、准确、真实和正确的，可供SZCA检查和核实；并且，愿意承担任何提供虚假、伪造等信息的法律责任。

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

- 用于证书中所含公钥相对应的私钥所进行的每一次签名，都是订户自己的签名，并且在进行签名时，证书是有效证书并已被订户接受（证书没有过期、挂起或撤销）。

- 未经授权的人员从未访问过订户私钥。
- 订户向发证机构陈述的所有包含在证书中的有关信息是真实、完整的。
- 就订户所知道的或注意到的包含在证书中的信息，都是真实的。如果订户发现了证书中信息存在某些错误，但订户还没有及时通知给发证机构，那么，发证机构认为：订户认为上述信息都是真实的。
- 证书将按本CPS 的规定，只用于经过授权的或其它合法的使用目的。
- 除非经订户和发证机构间的书面协议明确批准，订户保证不从事发证机构（或类似机构）所从事的业务，例如：把与证书中所含的公钥所对应的私钥用于签发任何证书（或认证其它任何形式的公钥）或证书撤销列表。
- 一经接受证书，既表示订户知悉和接受本CPS 中的所有条款，并知悉和接受相应的订户协议。
- 一经接受证书，订户就应承当如下责任：即始终保持对其私钥的控制，使用可信的系统，和采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用。
- 一经接受证书，订户即同意使SZCA免于由下列原因直接或间接造成的任何责任和损失：订户（或其授权的代理人）虚假地或错误地陈述了事实；订户未能披露重要事实，而订户的这种有意或无意的错误陈述或失职造成了对SZCA和任何信任其证书的人的欺骗；订户没有使用可信系统或没有采用必要的合理措施防止其私钥被损害、丢失、泄露、被篡改或被未经授权使用。如果因此给SZCA造成任何责任、损失、任何诉讼及一切费用，订户将予以经济赔偿。
- 作为证书申请者，有责任就申请代理人的疏忽和错误陈述及时通知证书签发者。

9.6.4 依赖方的陈述与担保

依赖方在信赖任何SZCA签发的证书时，就意味着保证：

- 熟悉本CPS的条款以及和所信赖订户证书的证书政策，了解证书的使用目的。
- 依赖方在信赖SZCA签发的证书前，已经对证书进行过合理的检查和审核，包括：

检查SZCA公布的最新的CRL，以获得该证书的状态，只有确认该证书没有被撤销时，SZCA才保证该证书是有效的；检查该证书信任路径中所有出现过的证书的可靠性；检查该证书的有效期以及适用范围。

- 一旦由于疏忽或者其它原因违背了合理检查的条款，依赖方愿意就此对SZCA带来的损失进行补偿，并且承担因此造成的自身或他人的损失。

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

9.6.5 其它参与者的陈述与担保

不适用

9.7 担保免责

除非在本CPS9.6.1中明确承诺外，SZCA不承担其它任何形式的保证和义务，同时SZCA将：

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

2. 订户违反本CPS9.6.3之承诺时，或者证书依赖方违反本CPS9.6.4之承诺时，得以免除SZCA的责任；

3. 不对电子认证活动中使用的任何软件做出保证。

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

5.SZCA只在证书有效期内承担赔偿责任。

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

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

9.8 有限责任

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

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

1. 个人类证书，不超过800元；

2. 单位类证书，不超过4000元；

3. 设备类证书，不超过8000元。

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

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

9.9 赔偿

在签发证书时，未按照本CPS的规定进行操作，或者违反法律法规的要求而造成证书订

户损失的；SZCA承担如CPS9.8所述有限赔偿责任。

有下列情形之一的，订户或依赖方应承担相应的损失赔偿责任：

- 订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致造成SZCA、注册机构或者第三者遭受损害的。
- 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知SZCA，以及不当交付他人使用造成SZCA、第三方遭受损害的。
- 订户使用证书或者依赖方信任订户证书，有违反本CPS及相关操作规范，或者将证书用于非本CPS规定的其它业务范围的。
- 用户使用或信赖证书时，未能依照法律法规、本CPS及其他规范及服务协议等的规定进行合理审核或履行合理的注意义务，导致SZCA或第三方遭受损害的。
- 证书订户或者其它有权提出撤销或挂起证书的人提出撤销或挂起请求后，到SZCA实际完成撤销或挂起该证书结束的期间，如果该证书被用以进行非法交易，或者进行交易时产生纠纷的，如果SZCA按照本CPS的规范进行了有关操作，那么该证书订户必须承担所有损害赔偿责任。
- SZCA与之签署的协议另有赔偿规定的，从其规定。

9.10 有效期和终止

9.10.1 有效期限

本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，最新版本可访问SZCA网站获得，对具体个人不做另行通知，当新版本正式发布生效，旧版本将自动终止。

9.10.2 终止

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

9.10.3 效力的终止与保留

在本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，如短信、电话、电子邮件、信函、传真等，个别通知订户、依赖方。

9.12 修订

9.12.1 修订程序

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

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

具体修订程序详见本CPS1.5.4“CPS批准程序”。

9.12.2 通知机制和期限

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

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

所有以书面形式提供给订户的CPS修订，按以下规则发送：

- 接受者是公司或其它单位组织向其登记联系地址或办公室发送信息。
- 接受者是个人向其申请书上规定地址发送。

- 这些通知可能用快递或挂号信的方式发送。
- SZCA可以选择通过电子邮件或其它方式向订户发送通知，邮件地址在订户申请证书时已注明。

9.12.3 修订同意

对于非重大修订，无需经各参与方同意，修订后CPS将在发布之时即生效。

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

9.12.4 必须修改业务规则的情形

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

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

9.13 争议处理

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

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

9.14 管辖法律

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

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

9.15 与适用的法律的符合性

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

9.16 一般条款

9.16.1 完整协议

本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。

9.16.2 转让

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

除以上原因外，SZCA、订户及依赖方之间的责任和义务不得以任何形式转让。

9.16.3 分割性

本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 其余的部分仍然有效。相关当事人了解并同意，SZCACPS所规定的责任限制、保证或其它免责条款或限制、或损害赔偿的排除等，均可独立于其它条款的个别条款，并可加以执行。

9.16.4 强制执行

不适用

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、地震、火灾、疫情、洪水、冰雹等；

（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）互联网或其他水电基础设施无法使用。

9.17 其它条款

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

附录二

版本信息

文档名	深圳CA电子认证业务规则	保密级别	公开

本文件历史变更记录			
版本	**生效时间**	**发布者**	**修订说明**
V1.0	2007.8	深圳CA	创建本CPS
V2.1	2012.12	深圳CA	联系方式变更，CPS管理机构变更，域名变更，词汇定义描述，证书费用说明，表达方式统一等
V3.0	2017.09	深圳CA	3.2.2组织机构身份的鉴别的方式进行了调整,增加了网上申请方式与证书用于内部环境时的申请方式。同时还增加了辅助信息的来源渠道。 3.2.3个人身份的鉴别,对相关证件的名称进行了调整。同时增加了在线认证方式。 3.2.6 对互操作准则进行补充说明。 4.1.3注册过程与责任增加在线申请的方式。 4.12密钥生成、备份与恢复中增加了云证书服务。 5.1.4水患防治中增加了水浸自动报警。 5.2.4 需要职责分割的角色。明确录入员和审核员不能由同一人担任。 6.2 私钥保护和密码模块工程控制。修改私钥的备份操作必须2人或以上才可完成。
V3.1	2018.05	深圳CA	增加3.2.4电子邮件鉴别，3.2.5设备鉴别
V3.6	2021.12	深圳CA	4.1.1 增加证书类型及其定义 4.12.1 更正密钥协同证书密钥生成描述 9.4.1、9.4.5 更新信息使用授权相关内容
V3.7	2022.10	深圳CA	主要对第三章身份标识与鉴别与第四章证书生命周期操作要求，按业务实际调整细化； 增加标识证书类型，调整更新自定义证书扩展项； 修正其他章节对应的证书主体名称、证书密钥生成传递相关内容； 其他文字性调整，及错误表述更正
V3.8	2024.6	深圳CA	更新公司地址、联系方式相关信息，及机房的分区及机房访问方式