SZCA

电子认证业务规则

深圳市电子商务安全证书管理有限公司

二〇〇七年八月

SZCA CPS

电子认证业务规则

SZCA Certification Practices Statement

(CPS)

版本1.0

发布日期： 2007年8月29日

生效日期： 2007年8月29日

深圳市电子商务安全证书管理有限公司

深圳市南山区高新中二路深圳软件园8栋301

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。

对任何复制本文件的其它要求，请和深圳市电子商务安全证书管理有限公司联系。

地址：中华人民共和国广东省深圳市南山区高新中二路深圳软件园8栋301室；

邮政编码：518057

电话：0755-26588399；

传真：0755-26588399-881；

电子邮件：CPS@szca.gov.cn

本CPS的最新版本请参见本公司网站http://www.szca.gov.cn，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数字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数字认证服务的个人、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、证书的吊销和公布、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数字签名、证书及CPS文件，证书申请者可以参加相关的培训和学习。
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（http://www.szca.gov.cn）。
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：CPS@szca.gov.cn。或请邮寄至：中华人民共和国广东省深圳市南山区高新中二路深圳软件园8栋301室（邮编：518057）

目 录

1. 概述性描述

1. 概述

1. 深圳市电子商务安全管理有限公司（SZCA）

深圳市电子商务安全证书管理有限公司,即深圳市电子证书认证中心，简称深圳CA中心、深圳CA，或者SZCA，成立于2000年8月，是一家第三方电子认证服务机构。SZCA按照《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，向公众（包括政府机构、企事业单位及个人）提供身份认证和信任服务。SZCA将严格按照信息产业部、国家密码管理局等主管部门的要求从事运营服务。

SZCA遵循 PKI 体系标准，为网络用户提供网上身份认证和信任服务，为保证网络活动双方身份的真实性、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。
SZCA与SZCA授权建立的操作子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第三方电子认证服务机构的服务主体。

SZCA提供认证服务，旨在建立网上交易和网上作业的互信，本CPS阐述的内容，在于规范证书整个生命周期的业务操作，保证服务能够完整、全面贯彻执行。作为被信任的第三方电子认证服务机构，SZCA及其授权的服务机构承诺，在证书有效的情况下，保证证书能唯一地与身份明 确的实体相关联，公钥能与身份确定的实体唯一相对应。

2. 电子认证业务规则（CPS）

本CPS详细阐述了SZCA签发和管理证书以及运营维护证书服务的设施的活动，并提供实际工作运营中应该遵守的规范。为SZCA电子认证服务安全性、规范性、可靠性和可操作性提供保证。

2. 文档名称与标识

1. 文档名称

本文档名称为SZCA电子认证业务规则，是深圳市电子商务安全证书管理有限公司对所提供的认证及相关业务的全面描述。

“SZCA CPS”、“深圳CA电子认证业务规则”、 “深圳CA CPS”、“深圳CA中心CPS”、“深圳CA中心电子认证业务规则”及其类似表述，无论在任何场所，均应被视为指称本文档或对本文档的引用。

本电子认证业务规则为SZCA 发布的第一个版本，是依据电子认证服务管理办公室《电子认证业务规则规范》（试行）、在原《SZCA安全管理策略和规范》和《SZCA对外运营策略和规范》的基础上修改整理。SZCA将会根据第三方认证业务的发展更新，更新的版本有注明版本号。

2. SZCA 标识

深圳市电子商务安全证书管理有限公司，即深圳市电子证书认证中心，缩写形式为SZCA，本文件所涉及的“深圳CA”、“SZCA”等是指深圳市电子商务安全证书管理有限公司。

SZCA 所拥有的品牌的商标为：

3. 电子认证活动参与者

1. 电子认证服务机构

SZCA 和SZCA下属的子 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方颁发数字证书。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。

SZCA 是所有SZCA 下层机构和实体的根。在十分严密的保密和安全机制控制下，SZCA 根据根证书有效的安全策略，根据国家密码管理局的有关规定，使用国家信任源根CA证书和由根CA签发的

SZCA证书。SZCA根据授权和协议，签发下一级的证书。SZCA　将决定在什么时间，什么地点、由什么人监督、怎么实施SZCA 根密钥对的变更和切换。

SZCA所签发证书，与每一个证书申领实体的公钥绑定。SZCA承诺，以签发、在有效期内的证书，将采用证书目录服务期和证书吊销列表（CRL）服务器，公布该证书的公开信息和状态。
SZCA 将建立完善的安全机制，以保证运营根私有密钥的安全性。在时机成熟的时候，SZCA 将建立异地备份中心。

2. 注册机构（Registration Authority）

SZCA的注册机构是经SZCA正式授权后的业务分支机构，主要功能是识别、鉴证证书申请者的实体，具体实施发起证书申请、吊销证书申请、更新证书申请等职能。

3. 受理点（Business Terminal）

经过SZCA 审查，SZCA 授权特定单位或实体，负责办理和审批数字证书申请手续，过程和要求，必须与SZCA 正在实施的电子认证业务规则以及SZCA 的 CA 受理点授权协议书相一致。受理点负责向SZCA 授权的注册机构或SZCA 授权的注册分支机构提供证书申请实体的信息，包括申请实体的名称、可以表明身份的证件号码和联系方法（通信地址、电子邮件信箱、　电话等）。受理点根据这些信息为申请实体制作证书或根据申请实体的要求，提供申请实体自行申请的技术支持。

4. 订户（Subscriber）

订户，即证书持有人，是指从SZCA接受证书的实体。包括已经申请并持有SZCA签发的数字证书的个人、单位、服务器、网站等提供网上服务和享受网上服务的各种实体，以及其它任何具有确定的身份标识，并持有SZCA签发的各类证书的人、物或组织单位。

5. 依赖方（Relying Party）

在SZCA证书服务体系范围内，任何使用证书进行网上作业的订户，以及按照SZCA　CPS合理信任证书真实性的任何实体，称为SZCA的依赖方。依赖方可以是、也可以不是一个订户。

依赖方应合理的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，依赖方必须在得到这些保证后才能合理的信任该数字签名。

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

保障，以及本CPS中涉及的权益。

6. 证书申请者（Certificates Applicant）

每一个期望成为SZCA或其下级子CA的订户的实体，都可以成为SZCA的证书申请者，根据其想要获得的证书类型，按照本CPS的规定提供必要的信息，完成申请过程。

证书申请者可以是个人、企业和其它任何组织机构。

7. 证书垫付商

指能够为其所属或所服务的订户或潜在订户群体承担所有证书服务费用的团体或组织，是一种特殊的证书服务受理点。证书垫付商根据本CPS的规定、SZCA公布的其它规定和法律、政策要求的情况，有权取缔由其支付费用的证书持有者的全部或部分证书服务，包括但不限于对持有者的数字证书的取消。

8. 其它参与者（Other Participants）

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

4. 证书应用

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、企业信息化、网上信息传递等多个领域的应用，为建设网络信任环境提供了基础性的信任服务。详细信息请参阅 http://www.szca.gov.cn/。证书申请者、订户和依赖方等各类主体可以根据时机需要，自主判断和决定采用相应合适的证书种类，以及了解证书的应用类型、应用范围，选择自己的应用方式。

SZCA签发的证书，从功能上可以满足下列安全需要：

- 身份认证-保证采用SZCA的证书持有者身份的真实性；
- 信息完整性-采用SZCA证书进行加密/数字签名时，可以验证信息在传递过程中是否被篡改，发送和接收信息是否完整一致；
- 数字签名-对数字签名的有效性可以进行验证。

2. 限制的证书应用

SZCA签发的证书禁止的应用范围包括：

1. 根据《中华人民共和国电子签名法》第三条规定，民事活动中的合同或者其它文件、单证等文书，当事人可以约定使用或者不使用电子签名、数据电文、当时人约定使用电子签名、数据电文的文书，不得仅因为其采用电子签名、数据电文的形式而否定其法律效力，前款规定不适用以下文书：
   a) 涉及婚姻、收养、继承人等人身关系的；
   b) 涉及土地、房屋等不动产权益转让的；
   c) 涉及停止供水、供热、供气、供电等公用事业服务的；
   d) 法律行政规定的不适用电子文书的其它情形。
2. SZCA与订户约定的证书禁止应用范围。
3. 证书禁止在任何违反国家法律、法规或破环国家安全的情形下使用，否则由此造成的法律后果由用户自己承担。

1. 策略管理

1. 策略文档管理机构

根据《中华人民共和国电子签名法》、《电子认证服务管理办法》和电子认证业务规则规范要求，SZCA制定本电子认证业务规则（CPS），并指定机构SZCA运营安全管理小组作为策略的最高管理机构。

SZCA运营安全管理小组作为SZCA电子认证服务所有策略的最高管理机构，由SZCA管理人员，组织PKI技术人员和法律顾问组成，负责审核批准CPS，并作为CPS实施检查监督的最高决定机构。

2. 联系人

SZCA 将对电子认证业务规则进行严格的版本控制，并由SZCA 指定专人负责。任何有关CPS的问题、建议、疑问等，都可以与此联系人进行联系。

联系人：深圳市电子商务安全证书管理有限公司办公室

电话：0755-26588399

传真：0755-26588399-881

地址：深圳市南山区高新中二路深圳软件园8-301

邮编：518057

电子邮件：cps@szca.gov.cn

3. 决定CPS符合策略的机构

按照信息产业部发布的《电子认证业务规则规范》要求，SZCA制定本电子认证业务规则（CPS），并提交信息产业部备案。SZCA运营安全管理小组作为策略的最高管理机构，是CPS符合策略的决定机构。

SZCA保证制定和发布的CPS，其执行、解释、翻译和有效性均符合和适用中华人民共和国的法律规定。

4. 电子认证业务规则批准程序

在SZCA 的CPS起草拟订后，提交SZCA运营安全管理小组审核。如果需要对电子认证业务规则做出变更，SZCA将草拟变更文本，提交SZCA运营安全管理小组会审核。经过该小组审议通过后，SZCA在网站http://www.szca.gov.cn公布变更后的SZCA 电子认证业务规则正式文档。

根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定，SZCA在CPS公布之日起三十日内向信息产业部备案。

2. 定义和缩写

1. SZCA

深圳市电子商务安全证书管理有限公司的缩写。

2. 电子认证服务机构(Certificate Authority, CA)

SZCA 及子CA统称为电子认证服务机构。

3. 注册机构

CA 注册机构简称 RA。与SZCA 签署注册机构协议， 被SZCA 授权发行SZCA 证书的代理机构。注册机构负责处理证书申请者提出的证书申请信息，并提交 CA。

4. 受理点

简称 LRA，与SZCA 签署受理点协议，被SZCA 授权发行SZCA 证书的代理机构，其功能比注册机构小。

5. 发证机构

包含SZCA 授权的注册机构、注册分支机构、受理点证书发放机构。发证机构为证书申请者发放SZCA 证书。

6. SZCA 运营安全管理小组

由SZCA 任命的负责SZCA 安全策略制定及执行的组织。

7. SZCA 超级管理员

负责实施 CA 政策、增加新 CA管理员、验证审计记录、电子认证业务规则的执行情况承诺。

8. 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。

9. SZCA 录入员

负责录入证书申请者提交的信息。

10. SZCA 审核员

负责审核证书申请信息。

11. SZCA 审计员

CA 审计员（Auditor）负责 CA 系统的证书统计，系统审计。

12. SZCA 证书制作员

负责为证书申请者制作下载证书。

13. 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。

14. SZCA 白皮书

SZCA 白皮书是SZCA 的一个支持SZCA 数字证书相应政策的详细的操作 规则和操作步骤。

15. 注册机构协议

一份合同，它详细地概括了SZCA 指定的注册机构的程序、责任和义务。

16. 注册分支机构协议

一份合同，它详细地概括了SZCA 指定的注册分支机构的程序、责任和义务。

17. 受理点协议

一份合同，它详细地概括了SZCA 指定的受理点的程序、责任和义务。

18. 依赖方

依赖方（Relying Party）指基于对数字证书和/或电子签名的信任而从事有关活动的人。

19. 订户

个人、集体、单位、组织、服务器或者其它拥有任何SZCA 证书的人或实体。

20. 证书申请者

证书申请者（Certificate Applicant）请求SZCA 颁发证书的个人、企业、组织 机构。

21. 用户

用户（Subscribers）指由 CA 深圳签发的各种类型证书的持有者。

22. 终端用户

SZCA 中的终端用户包括所有证书申请者、终端管理员和操作人员及要求数 字证书验证和加密服

务的系统和服务器。所有终端用户由SZCA 授予证书，并且 是证书的主体。终端用户可以使用SZCA 授予的证书为其它终端用户加密信息， 也可校验其它终端用户的电子签名。这样，终端用户也可是SZCA 中的可信赖方。

23. 证书申请

由证书申请者提交给SZCA 的请求，SZCA 根据此请求为用户颁发证书。

24. 参考码

SZCA 为证书申请者颁发证书时生成的 32 位字符组合。唯一标识证书申请。 与授权码相对应。

25. 授权码

SZCA 为证书申请者颁发证书时生成的32位字符组合。与参考码相对应。

26. 证书口令

证书口令指证书中私有密钥的保护口令。

27. 证书序列号

唯一标识证书的 32 位字符组合。

28. 甄别名

甄别名（Distinguished Name）简称 DN，包含用户的属性信息。

29. 密钥管理中心

密钥管理中心简称 KMC，负责密钥的产生、存储、归档等工作。

30. 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。

31. LDAP

LDAP（Lightweight Directory Access Protocol），即轻量级目录访问协议， 用于查询、下载数字证书以及数字证书吊销列表（CRL）。

32. PKI

PKI（Public Key Infrastructure），公开密钥基础设施。

33. CRL

CRL（Certificate Rovocation List），即数字证书吊销列表的英文简称。CRL 中记 录所有在原定失效日期到达之前被吊销的数字证书的用户数字证书序列号，供数字 证书使用者在认证对方数字证书时查询使用。CRL 通常又被称为数字证书黑名单。 内容通常还包含 CA 机构的名称、发行日期、下次吊销列表的预定发行日期、变更 或吊销的数字证书序号，并说明变更或吊销的时间与理由。

34. 认证

认证（Certification）指不同实体在进行网上交易之前，通过可信赖的、中立的第三方（如SZCA）对身份进行审核，并由第三方出具证明证实其身份的可靠性和合法性的过程。

35. 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。

36. 私有密钥

私有密钥（Private Key），是一种不能公开、由持有者秘密保管的数字密钥， 用于创建电子签名、解密报文或与相应的公开密钥一起加密机要文件。

37. 公开密钥

公开密钥（Public Key），可以公开的数字密钥，用于验证相应的私有密钥签名的报文，也可以用来加密报文、文件，由相应的私有密钥解密。

38. 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。

39. 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。

40. PKCS

PKCS （Public Key Cryptography Standard），公开密钥密码算法标准。

41. HTTP

HTTP （Hypertext Transfer Protocol），超文本传输协议。

1. 信息发布与信息管理

1. 认证信息的发布

SZCA的电子认证业务规则、订户责任书及公告通知等可以从SZCA的网站http://www.szca.gov.cn获取；用户证书可以从SZCA的LDAP上获取；已被吊销的证书信息可以从CRL站点、LDAP查获，而证书的状态（有效、吊销、挂起）可通过OCSP获得。

SZCA的 网站http://www.szca.gov.cn、LDAP、CRL及OCSP服务器构成了SZCA认证信息发布的信息库。SZCA将及时公布新的信息，处理旧的信息。

信息库的发布及更改一律须经SZCA 核准。如有需要可访问SZCA 网站http://www.szca.gov.cn 查看。

2. 发布时间或频率

1. 电子认证业务规则的发布时间及频率

SZCA将及时发布电子认证业务规则（CPS）的最新版本。一旦对规则的修改、补充等获得批准，SZCA将在www.szca.gov.cn上发布，其发布时间及频率由SZCA 决定。

2. 证书及CRL的发布时间及频率

一旦订户接受证书，SZCA将在信息库上和有其指定的其它一个或多个信息库里发布该证书。证书通过目录服务器发布时，SZCA将在成功签发证书的同时进行实时发布。用户可在SZCA网站http://www.szca.gov.cn/上查询或下载数字证书。

所有被吊销或挂起的证书，其列表CRL通过SZCA的目录服务器自动发布。根据需要，也可人工发布最新CRL。用户可在SZCA网站http://www.szca.gov.cn/上查询或下载最新的CRL。CRL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. 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将在第一时间在其网站http://www.szca.gov.cn 上进行发布。

3. 信息库访问控制

每个SZCA的万维网URLs均可以采用带有安全套接层协议（SSL）的超文本传输协议（HTTP），以实现访问记录的安全模式，其它发布重要信息的万维网URLs也采用https方式进行。

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 在线的公告版本和公布信息。经过授权的操作要留有操作记录。

SZCA 在必要时可自主选择并实行信息的权限管理，以确保只有证书用户才有权阅读受SZCA 控制的信息资料。

2. 身份标识与鉴别

1. 命名

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，采用X.500 标准命名方式。

CA颁发机构主体甄别名

属性	值
国家（C）	CN
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

最终订户证书主题甄别名命名规则

属性	值
国家（C）	CN
通用名（CN）	属性包括： 域名（服务器证书），或 组织机构名（机构身份证书），或 个人姓名（个人证书），或
机构（O）	证书订户所在的机构的机构名称 或不填
机构部门（OU）	可以包含以下一个或多个内容： 订户的组织机构部门

	一个引用依赖方协议的声明，该依赖方协议明确了使用证书的条款。 版权通告 描述证书类型的文字
城市（L）	订户所在城市
省份（ST）	订户所在省份或不用
电子邮件（E）	订户的电子邮件地址

2. 对名称意义化的要求

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

3. 订户的匿名或伪名

本CPS明确声明，SZCA不接受或者允许任何匿名或者伪名，仅接收有明确意义的名称作为唯一标识符。

4. 理解不同名称形式的规则

SZCA颁发的证书中，证书的主体包含有用户的甄别名（Distinguished Name），是唯一标识证书用户的身份。SZCA 证书符合 X.509 标准，甄别名格式遵守 X.500 标准。

甄别名的命名规则由SZCA定义。

5. 名称的唯一性

SZCA的所有证书持有者，证书主体必须是唯一的。当DN项相同时，遵循先申请者优先使用此DN项，后申请者在DN项增加附加识别信息加以区别的原则。

6. 商标的识别、鉴别和角色

SZCA签发得证书主题甄别名中将不包含商标名。

2. 初始身份确认

1. 证明拥有私钥的方法

SZCA在证书签发时，根据证书申请信息中的信息，SZCA首先利用数据摘要算法进行计算，再用申请信息中的公钥对申请信息中的私钥解密，然后进行比较，如果相等则证明数字证书的申请者拥有与签名公钥对应的签名私钥。

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，在证书申请书上签字表示接受证书申请的有关条款， 并承担相应的责任。SZCA及其证书服务机构当面审核单位证书申请者的代表人是否符合要求。

对组织机构的身份鉴别按以下方式进行：

1. 组织机构授权办理人携带本人身份证原件、机构工商营业执照登记证、组织机构代码证原件（正本或副本）及复印件亲自到证书申请现场。
2. 核对办理人身份证、机构工商营业执照登记证、组织机构代码证原件（正本或副本）与复印件是否一致。
3. 核对办理人身份证、机构工商营业执照登记证、组织机构代码证信息与申请表相应信息是否一致。
4. 确认组织机构接受SZCA“数字证书用户责任书”中的各项条款。
5. 检查订户提交申请材料的完整性。
6. SZCA可以通过查询第三方数据库或咨询相应的政府机构等方式，并通过电话、邮政地址调查等SZCA以为合理的方式辅助进行鉴别。
7. 如果SZCA无法从第三方得到所有需要的信息，可要求第三方进行调查，或要求证书申请者提供额外的信息和证明材料

申请者必须保证所有材料的真实性，SZCA和其授权的证书服务机构将对申请者的材料按照法律规定进行审查

1. 个人身份的鉴别

SZCA 授权发证机构查验人员合理、谨慎地核对申请资料的原件与复印件， 根据查验人员的管理

规定对申请者的资料的真实性进行审查，并进行批准或拒绝的操作。

SZCA在接到个人订户的证书申请后,向该订户签发证书前,必须对该证书申请者的个人身份进行查验和鉴别,鉴别要求如下:

1. 个人证书申请者携带本人身份证或护照原件及复印件亲自到证书申请现场，通过面对面的核实方式确认该订户的真实身份。
2. 核对申请者身份证或护照原件与复印件是否一致。
3. 核对申请者身份证原件或护照与申请表相应信息是否一致。
4. 确认该申请者接受SZCA“数字证书用户责任书”中的各项条款。
5. 检查该订户提交申请材料的完整性。

申请者必须承担材料真实性的责任，SZCA和其授权的证书服务机构在进行了法律规定的有限审查以后，不承担对申请者的身份证明，如身份证等进行合法性甄别的义务。
SZCA 和其授权的证书服务机构保存证书持有者在申请表中填写的详细信息。

2. 域名（或IP地址）的确认和鉴别

申请者填写书面申请表，经过单位授权代表的签署及单位盖章后（如为个人申请则需要个人签名），携带相关资料到SZCA 授权的发证机构进行身份查验及办理交费手续。

如果证书的甄别名（DN）为域名 (RDN)，除了在对申请者递交的书面材料进行审核外，SZCA可能需要申请者提供额外的域名使用权证明材料，或向相应的域名注册服务机构查询，以确定订户是否有权使用相应的域名。

SZCA 授权的发证机构的审核人员合理、谨慎地核对申请资料的原件与复印件，根据查验人员的管理规定对申请者资料的真实性进行审查。

3. 没有验证的订户信息

对于没有验证过的申请者信息，SZCA将以书面的形式进行归档，并不为该申请者签发任何形式的证书。SZCA将不承诺申请者这类信息的真实性，并且不承担由于这类信息的不真实、不完整等引起的任何责任和纠纷。

4. 授权确认

在组织机构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申请代表人的身份和资格，包括代表人的身份资料和授权证明，并且可以通过电话、信函或其它方式与其代表的组织机构进行核实确认，以审核他是否有权代表那个组织机构。

SZCA可以通过第三方或其它方式确认授权申请人的信息。如果不能确认其信息，可以要求证书申请者提供额外的信息证明材料。

5. 互操作准则

对于非SZCA的其它机构，如果双方之间有协议，那么SZCA将依据协议的内容，接受该机构鉴别过的信息，并为之签发相应的证书。如果双方没有任何类似的协议，SZCA要求该机构要严格按照本CPS的规定鉴别身份信息。SZCA会根据情况决定是否接受这些被鉴定审核过的材料，并作出是否接受受理的决定。

如果国家法律法规对此有规定，SZCA将严格予以执行。

1. 密钥更新请求的标识与鉴别

一般情况下，证书的有效期为一年。根据情况，SZCA可以决定证书有效期长短。到期后密钥需要更新，并向发证机构申请重新签发证书。

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。

1. 常见密钥更新的标识与鉴别

对于证书有效期结束后的常规密钥更新，证书拥有者可以使用原有的私钥对更新请求信息签名，提出重新签发证书申请。发证机构将会对更新请求信息进行正确性、合法性、唯一性的验证和鉴别，后签发新证书。

或者，证书用户申请变更证书或密钥时，填写变更申请表按照初始身份验证步骤提交相关资料并由SZCA 授权的发证机构查验。SZCA 授权的发证机构的查验人员合理、谨慎地核对申请资料的原件与复印件，根据查验人员的管理规定对申请者的资料的真实性进行审查，决定批准或拒绝。

2. 吊销后密钥更新的标识与鉴别

发证机构不提供证书被吊销后的密钥更新。证书用户必须重新进行身份鉴别和注册，申请新的证书。

2. 吊销请求的标识与鉴别

证书的吊销请求，需要到SZCA的证书服务机构办理，证书用户申请吊销证书时，填写证书吊销申请表，照初始身份验证步骤提交相关资料并由SZCA 授权的发证机构查验。

SZCA 授权的发证机构的查验人员合理、谨慎地核对申请资料的原件与复印件，根据查验人员的管理规定对申请者的资料的真实性进行审查，决定批准或拒绝。

1. 证书生命周期操作要求

SZCA以及授权发证机构提供数字证书授权、申请、发放、变更、查询和管理等服务，为订户提供网络信息安全及身份认证、电子签名、密钥管理等与数字证书密切相关的配套服务。本章节描述的证书包括 CA 系统管理员证书、系统模块通讯证书、订户证书等。本章节主要以订户证书中的证书申请者为模板，描述证书处理流程及业务规范。

1. 证书申请

1. 证书类型

目前，SZCA提供正式证书和测试证书两种类型。

1. 测试证书

对于测试证书， SZCA不承担任何证书真实性的责任，仅供用户测试使用，SZCA建议用户不要将测试证书应用到任何需要证明真实身份的场所，以免引起不必要的损失和纠纷。

申请者通过提交一些简单的信息后，就可以获得测试证书。这些填写的信息， SZCA不对信息进行保存或者公布，也不承担因为申请者填写的信息泄漏引起的任何责任。

2. 正式证书

正式证书是指申请者按照本CPS的规定和流程，递交真实的申请信息后经过认证机构批准获得证书，SZCA对此类证书承担本CPS规定的义务和责任。证书申请者根据申请的证书种类，提交内容完整的带个人手写签名或者加盖公章的申请表格。该申请表可以从SZCA的网站下载或到SZCA和其授权的证书服务机构领取。证书申请表格的填写内容，依照申请证书类型的不同而不同。

1、个人证书

SZCA的个人证书是经SZCA签名的包含个人身份信息以及个人公钥的文件，证书的格式遵循x.509国际标准。它用于标志证书持有人在进行信息交换、电子签名、电子政务、电子商务等网络活动中的身份，并且保障信息在传输中的安全性和完整性。

申请者申请个人证书，需要递交以下资料：

- 申请者填写并签字的书面申请表
- 个人身份证（或军官证、或护照等）原件
- 个人身份证（或军官证、或护照等）复印件
- 如果是委托办理，需同时递交申请人和被委托人的上述证件及复印件，以及申请委托人亲笔签名的书面授权书。

2、单位证书

单位证书，SZCA的单位证书中包括企业基本信息、企业的公钥及SZCA的签名，颁发给独立的企事业单位、政府部门、社会团体等各类组织机构。在互联网作业中，它可以证明证书持有者的身份。

申请单位证书，需要递交以下资料：

- 申请者填写并签字盖章（加盖国家认可的公章）的书面申请表
- 申请者的企事业单位组织机构代码证的原件（正本或者副本）及加盖国家认可的公章的复印件
- 申请者的营业执照原件（正本或者副本）及加盖国家认可的公章的复印件，如果没有营业执照，则提供书面申请表上可选的其它有效证件原件（正本或者副本）及加盖国家认可的公章的复印件；目前认可的有效证件如下：
    - 工商营业执照
    - 事业单位法人登记证
    - 税务登记证
    - 组织机构代码证
    - 社会团体登记证
    - 政府批文
    - 以及其它国家法律承认有效的证明文件。
- 受托申请人的身份证（或军官证、或护照等）原件与复印件
- 申请者对受托申请人的书面委托授权书（需加盖国家认可的公章）

3、设备证书

（a）服务器证书

申请服务器证书，需要递交以下资料：

- 申请者填写并签字（或盖章）的书面申请表（一式三份）
- 申请者（个人或组织机构）的身份证明材料原件和符合条件的复印件（具体要求同前述个人和单位证书的要求）。

- 该Web域名（或IP地址）所有者的ICP准营证或者政府主管部门网站备案说明。
- 如果是委托办理，需同时递交申请者和受托人的身份证明文件及复印件，以及申请者亲笔签名的书面授权委托书。

（b）代码签名证书

SZCA目前只提供单位代码签名证书：

代码签名证书，以单位身份申请的代码签名证书，用于对软件代码—如宏、病毒更新、.exe，.dll，.cab，.ocx等后缀文件等进行签名，以有效防止其软件代码被篡改，拥有者身份被冒用等。下载经过代码签名的软件时，可以确保软件的来源和软件的完整性。

申请单位代码签名证书，需要递交以下资料：

- 申请者填写并签字盖章（加盖国家认可的公章）的书面申请表申请者的企事业单位组织机构代码证的原件（正本或者副本）及加盖国家认可的公章的复印件
- 申请者的营业执照原件（正本或者副本）及加盖国家认可的公章的复印件，如果没有营业执照，则提供书面申请表上可选的其它有效证件原件（正本或者副本）及加盖国家认可的公章的复印件；目前认可的有效证件如下：
  - 工商营业执照
  - 事业单位法人登记证
  - 税务登记证
  - 组织机构代码证
  - 社会团体登记证
  - 政府批文
  - 以及其它国家法律承认有效的证明文件。
- 受托申请人的身份证（或军官证、或护照等）原件与复印件
- 申请者对受托申请人的书面委托授权书（需加盖国家认可的公章）

2. 证书申请实体

在证书申请的过程中，参与整个申请过程的实体主要包括：

1、 证书申请者，包含个人，企业单位、事业单位、政府机构、社会团体、人民团体等各类组织机构。任何合法的组织和个人和有明确身份归属的其它网络主体均可申请数字证书，以保证网上交易和网上行政作业的安全和可靠。

2、 注册服务受理机构，包括分中心RA、受理点LRA以及证书垫付商等。CA机构或RA机构的系统及相应的管理员。

3、 电子认证服务机构，包括SZCA以及SZCA授权的下一级操作子CA等。

4、 提出证书申请请求的各类主体。

5、 订户，申请并被通过的证书申请者，发证机构已经为其签发证书，他不依赖于用户是否已经接受证书。

6、 密钥生成器提供者，包括电子认证服务机构和用户自己选择的密钥生成器提供者，包括但不限于USB Key、加密卡、加密机等硬件提供者和IE等软件提供者。

7、 主管部门，包括中华人民共和国电子签名法、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的各类主管部门。

8、 目录服务

9、 依赖方

1. 注册过程与责任

4.1.3.1注册过程

证书证书离线申请流程

1、 证书申请者携带相关证明到各个证书服务机构的受理点LRA（或者通过邮递方式向受理点提出申请），填写相关申请表格。

2、 受理点LRA审核证书申请者和相关身份资料的真实性。如果身份鉴别未通过，受理点LRA将拒绝为用户发放证书，并将未通过的信息存档。

3、 如果身份鉴别通过，受理点LRA通过服务系统录入、审核证书申请信息，将信息递交给注册机构RA，由其转交给CA发证机构进行签发。

4□ SZCA在签发证书前，有权对证书信息进行二次审核，有权对身份审核不通过的订户拒绝签发证书

5、 对于签发成功的订户，受理点进行制证操作

6□ CA发证机构根据证书请求签发证书，并将证书及密钥存储在相应介质中。

7、 申请者领取存有证书及密钥的介质。

对于离线申请，SZCA要求：

申请者必须真实填写证书申请信息，并遵守《数字证书订户申请责任书》，否则SZCA 有权拒绝签发证书、停止证书的使用、吊销证书。由此造成的后果，SZCA 不承担责任。

SZCA和其授权的证书服务机构要求证书订户或者订户代表妥善保存申请资料和相关证明文件的复印件，保存期为证书失效后五年；直到申请人与SZCA终止合作为止，这种保存也需要保存至少5年；如果因为证书订户或者订户代表未按照要求保存资料，造成损失的，SZCA和其授权的证书服务机构不承担任何责任，如果这种未保存行为造成SZCA和其授权的证书服务机构损失的，

SZCA和其授权的证书服务机构保留相关的法律权力。

深圳CA目前暂不提供在线申请方式。

4.1.3.2 各参与实体的责任

1、 电子认证服务机构的责任

电子认证服务机构应承担的绝对的责任是：保证SZCA CA机构本身的签名私钥在SZCA内部得到安全的存放和保护，SZCA 建立和执行的安全机制符合国家相关政策的规定。

电子认证服务机构对其授权的证书服务机构进行审计和管理，保证整个申请过程的安全可靠。
电子认证服务机构保证整个CA系统安全可靠的运行。SZCA不对由于客观意外或其它不可抗拒事件造成的操作失败或延迟承担任何损失、损坏或赔偿责任。为了表达明确，这些事件包括罢工、暴动、骚乱或战争、火灾、爆炸、地震、洪水等大灾难。

由于技术的进步与发展，电子认证服务机构会要求证书订户及时更换证书以保证证书的可靠性。

2、 注册机构RA的责任

注册机构RA按照程序取得SZCA的授权，遵循本CPS和SZCA的授权运作协议和其它SZCA公布的标准和流程，接受并处理证书服务申请者的证书服务请求，并依据授权设置和管理各类下级证书服务受理机构，包括RA、LRA等。

RA必须遵循SZCA制订的服务受理规范、系统运作规范和管理规范，SZCA将不断的完善并及时发布有关的规范和标准内容。根据本CPS、SZCA公布的规范，RA有权决定是否给申请者提供相应的证书服务。

RA按照SZCA的要求和规范，确定下属证书服务受理机构的设置方式、管理方式和审核方式，这些方式的确定必须以书面的文件形式公布，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。

RA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必须能够提供证书服务全部的数据资料及备份，并按照SZCA的要求，保证其与下属证书服务机构间的信息传输安全。重要的是，RA承诺严格执行为所有证书用户提供资料的义务，并愿

意承担因此而带来的法律责任。

电子认证服务机构根据本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。CA具有对所有证书服务申请者服务请求的最终处理权。CA有权对申请者的资料进行复查；因为申请者的资格审核不严而导致的由证书使用引起的所有损失，由申请者承担。

3、 受理点LRA的责任

受理点LRA提供服务和本身的管理，必须遵守所有的登记程序和安全保障措施。这些程序和保障由SZCA公布和决定，并在本CPS和SZCA相应的授权运作协议中规定，以后SZCA可以根据情况修改有关内容，并及时公布。LRA同时还必须遵守其上级的CA、RA通过授权和协议所规定的内容。

LRA作为被授权的证书服务机构，需要接受授权机构对其进行的资格审核和管理检查。LRA对所有证书服务申请者真实性的信息鉴别负有责任，无论这种申请受理与否。

4、 垫付商的责任

垫付商必须承担其所有垫付的证书费用，并按SZCA规定的方式付清。

垫付商的垫付行为，就表明其愿意并且能够承担本CPS以及SZCA相关协议的规定，对证书服务申请者的身份真实性提供担保的责任。

5、 证书申请者的责任

证书申请者必须严格遵守与证书申请以及私钥的所有权和安全保存相关的程序：
证书申请者承诺，在证书服务申请表上填列的所有声明和信息必须是完整、精确、真实和正确的，可供发证机构检查和核实；并且，证书申请者愿意承担任何提供虚假、伪造等信息的法律责任。
证书申请者必须仔细阅读和服从所有本CPS罗列的或者由SZCA推荐或使用的安全措施，以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，需要熟悉本CPS的条例和与证书相关的证书政策，SZCA在接到证书申请者的任何服务申请前，都认为该持有人已经了解本CPS的内容，并承诺遵守证书持有者证书使用方面的有关限制。

6、 订户的责任

SZCA一旦通过证书申请者的申请并为其签发证书，无论是否已经接受证书，证书申请者就已事实成为证书订户。

订户必须确保本身持有的证书用于申请时预定的目的。

订户必须保证私钥的安全。当然SZCA只是提醒，并不要求证书申请者一定遵从SZCA要求的安全措施；订户可以选择任何自己认为可以保密的所有措施；同时，SZCA声明，SZCA并不承担因用户的私钥保存出现问题而带来的所有责任，除非订户能够合法的证明这种问题产生的主要责任在发证机构。

一旦发生任何可能导致安全性危机的情况，包括证书订户遗失私钥、遗忘或泄密以及其它未罗列的情况，证书订户应立刻通知SZCA CA机构、RA、LRA等各级证书服务机构，采取申请作废等处理措施，以保证订户的利益。

7、 依赖方的责任

依赖方在信赖任何SZCA及其下级操作子CA签发的证书的时候，必须保证遵守和实施以下条款：
依赖方熟悉本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作废时，SZCA才保证该证书是有效的；SZCA认为，依赖方一直是遵循了此条款的。一旦依赖方因为疏忽或者其它原因违背了此条款而给SZCA带来损失时，SZCA保留采取相应法律行为的权利。

所有依赖方必须承认，他们对证书的信赖行为就表明他们承认了解本CPS的有关条例包括有关免责、拒绝和限制义务的条款。

8、 目录服务的责任

SZCA在目录服务器上公布证书订户的证书和相关CRL。

SZCA周期性自动公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www.szca.gov.cn进行公布。

9、 密钥生成器提供者的责任

一旦证书申请者选择了某种密钥生成器，则表明该申请者信赖由其产生的密钥对的安全性和可靠性,SZCA并不为此提供任何形式的担保，也没有责任和权力对由此产生的纠纷进行处理。

10、 主管部门

SZCA承诺，将严格按照国家的法律法规和主管部门的书面要求提供符合要求的申请注册服务。

1. 证书审核

1. 证书申请的识别与鉴定

SZCA或授权的发证机构遵循第三章对证书申请者提交的信息进行审核。出于安全性和审计的需要，证书申请表应记录鉴别人的姓名、签名、验证结果和验证日期。

SZCA和其授权的证书服务机构的审核人员合理、审慎地进行申请者的身份鉴别，决定批准或拒绝。

2. 证书申请的通过与拒绝

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。

2. 证书申请的拒绝

如果申请者未能成功通过身份鉴别，SZCA将拒绝申请者的证书申请，被拒绝的证书申请者可再次提出申请。

身份审核失败时，SZCA有权拒绝解释，并且不需要通知申请者，法律法规对此有明确要求的除外。

3. 证书审核时间

SZCA 或授权的发证机构原则上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。

2. 证书签发

1. 签发证书

- 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；
- SZCA 授权的发证机构批准证书申请后SZCA 将为证书申请者颁发证书。并将有关资料一起提供给用户
- 证书的发行意味着SZCA 最终完全正式地批准了证书申请。证书从订户接受证书时起将被视为有效证书。

2. 证书签发通知

SZCA 直接通知订户或发证机构证书已签发。发证机构将证书及有关资料提供给申请者。

3. 拒绝签发证书

SZCA 授权的发证机构根据其独立判断，可以拒绝签发证书，并且不对因此而导致的任何损失或费用承担任何责任和义务。

3. 证书接受

1. 4.4.1 证书接受

在SZCA 数字证书签发完成后，SZCA 的发证机构将会把数字证书及使用资料等产品交给证书申请者，证书申请者从获得证书起就被视为已同意接受证书。证书申请者接受数字证书后，应妥善保存其证书对应的私有密钥（存放于存储介质中）。

2. 证书申请者陈述

一旦接受SZCA签发的证书，从接受之时起直至证书的整个使用有效期内，如果证书申请者不另行通知，那么证书申请者被视为向SZCA、发证机构及所有合理信赖证书中所含信息的个人、实体作出如下保证：

- 用于证书中所含公钥相对应的私有密钥所进行的每一次电子签名，都是证书申请者自己的电子签名，并且在进行电子签名时，证书是有效证书并已被证书申请者接受（证书没有过期、吊销）；
- 未经授权的人员从未访问过证书申请者私有密钥；
- 证书申请者向发证机构陈述的所有包含在证书中的有关信息是真实的；
- 就证书申请者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 证书申请者发现了证书中信息存在某些错误，但证书申请者还没有及时通知给发证机构，那么，发证机构认为：证书申请者认为上述信息都是真实的）；
- 证书将按SZCA 电子认证业务规则的规定，只用于经过授权的或其它合法的使用目的；
- 证书申请者是最终证书申请者，而不是发证机构。除非经证书申请者和发证机构间的书面协议明确批准。证书申请者保证不从事发证机构（或类似机构）所从事的功能，例如：把与证书中所含的公钥所对应的私有密钥用于签发任何证书（或认证其它任何形式的公钥）或证书吊销列表。

一经接受证书，既表示证书申请者知悉和接受SZCA 电子认证业务规则中的所有条款和条件，并知悉和接受相应的《数字证书用户申请责任书》里的所有条款。

3. 证书申请者责任

一经接受证书，证书申请者就应承担如下责任：始终保持对其私有密钥的控制，使用安全可信的系统，和采取合理的预防措施来防止私有密钥的遗失、泄露、被篡改或被未经授权使用。

4. 申请者的赔偿

一经接受证书，证书申请者即同意SZCA、SZCA 授权的发证机构以及他们的代理商、签约商对于由下列原因直接或间接造成的任何责任和损失不承担法律责任：

- 证书申请者（或其授权的代理人）虚假地或错误地陈述了事实；
- 证书申请者未能披露重要事实，而证书申请者的这种有意或无意的错误陈述或失职造成了对发证机构、SZCA或任何信任其证书的人的欺骗；
- 证书申请者没有使用安全可信的系统或没有采用必要的合理措施防止其私有密钥被损害、丢失、泄露、被篡改或被未经授权使用；

- 证书申请者对SZCA 和SZCA 授权的 CA 发证机构以及他们的代理商、签约商造成的责任和损失包括：由于上述原因直接或间接造成的责任、损失、任何诉讼、 仲裁及一切相关费用，包括但不限于诉讼费用、仲裁费用以及律师费等。对于由此发生的全部责任和损失，证书申请者将予以经济赔偿；
- 当证书是应证书申请者代理人的要求签发而给依赖方带来损失时，代理人应向发证机构、SZCA ，依照本节规定进行连带赔偿。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。

5. 发布

一旦证书申请者接受证书，发证机构将在目录服务器及由SZCA 和发证机构决定的其它一个或多个方式发布证书的副本。证书申请者也可以在其它资料库中公布其由SZCA 签发的数字证书。

4. 密钥与证书的使用

1. 订户私有密钥和证书的使用

证书应用范围：

证 书 种 类	证书应用范围
个人数字证书	符合X.509标准的数字证书，证书中包含个人身份信息和个人的公钥，用于标识证书持证者身份。数字证书和对应的私钥存储于Key中，用于个人在网上活动中标明身份，收发加密、签名邮件。
企业数字证书	符合X.509标准的数字证书，证书中包含企业信息和企业的公钥，用于标识订户的身份。数字证书和对应的私钥存储于Key中，可以用于企业等在电子商务、电子政务方面的活动，如合同签定、网上交易、网上工商、网上税务等方面。
服务器数字证书	符合X.509标准的数字证书，证书中包含服务器信息和服务器的公钥，用于标识该服务器的身份。
代码签名数字证书	符合X.509标准的数字证书，使用该证书对软件代码数字签名，用于表示软件代码的开发者身份。

2. 密钥及证书的使用说明

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（存于存储介质Usbkey中)，避免遗失、泄漏、被篡改或者盗用。任何人使用证书时都必须检验证书的有效性，包括该证书是否被吊销、是否在有效期内、是否是SZCA和其授权的发证机构签发等。

在使用与SZCA所签发的证书有关的签名及经过签名的信息时，参与方（SZCA和证书服务机构、证书订户和依赖方等）按本CPS的规定享有相应的权利和应尽的义务。参与方均视为已被通知并同意遵守本CPS以及SZCA与各方签署的协议、规范中的条款。任何超出本CPS的规定的证书及私鈅的使用，SZCA 将不承担由此带来的后果。

SZCA签发的各类证书，仅用于表明证书持有者在申请证书时所要标识的身份，以及验证证书持有者用于该证书内包含的公鈅相对应的私鈅做出的签名。这样，通过签名和签名的验证，保证证书持有者的身份真实性、信息的完整性、信息的不可抵赖性等。如果证书持有人将该证书用于其它用途，SZCA将不承担任何由此产生的责任和义务。

如果证书中的某些字段明确了证书的使用范围和用途，那么该证书将在也只被允许在这一范围内进行使用。任何超出证书所标明的适用范围内的行为，都将由行为人独立承担责任。SZCA对超出适用范围的任何使用行为，不承担任何由此产生的责任和义务。

3. 签名及验证

签名只限于以下几种情况下才能被创建：

- 在证书的使用有效期内被创建
- 该签名能通过对证书链的确认来正确验证
- 信赖方没有发现或注意到签名者违背SZCA CPS 要求的行为
- 依赖方遵守SZCA CPS 的所有规定。

证书的使用并不表示订户一方可以按任何个人的利益而行事或者有采取任何特殊行动的权力。进行签名的验证是为了确认签名是用签名者证书中所列的公钥相对应的私钥创建的,以及该签名创建后被签名的信息没有被更改过。

4. 依赖方证书和公钥的用途

获得对方的证书后，可以通过查看证书以了解对方的身份，通过公钥验证对方电子签名的真实

性，实现通信的不可抵赖性，并实现通信双方数据传输的保密性和完整性。

在信任证书和签名前，依赖方要独立地做出应有的努力和合理的判断。除非本CPS另有规定，证书并不是来自发证机构的对任何权力或特权的承诺。依赖方只能在本CPS规定的范围内信赖证书和证书中包含的公鈅，并对此做出决定。

如果证书中的某些字段明确了证书的使用范围和用途，那么该证书将在也只被允许在这一范围内进行使用。依赖方必须对此做出合理的判断，任何对超出证书所标明的适用范围的行为的信赖，都将由依赖人独立承担责任，SZCA对此不承担任何责任和义务。

5. 证书更新

为保证证书及其密钥对的安全有效，SZCA 会为签发的证书设置有效期，一般为一年。这也是为了保证证书订户的权利。证书订户必须在证书有效期到期前一个月内，到SZCA 授权的发证机构申请作更新证书处理。

1. 证书更新的情形

当证书持有者的证书有效期即将结束时，SZCA将作出合理的努力，在证书有效期满之前向证书订户或者证书委托人、证书申请时垫付商或者代理商发送证书更新提示；合理的努力包括但不限于网站提示、系统提示、书面提示、电话通知、E－mail通知或其它方式、但SZCA和其授权的证书服务机构采取了上述任何一项提示或通知方式，均可被视为进行了合理的努力。

经SZCA和其它授权的服务机构签发的用户证书有效期一般为一年，有效期从签发之日起计算。

同时，SZCA也接受订户自主提出的更新要求，对其证书进行更新处理。

2. 请求用户证书更新的实体

所有持有SZCA和其授权的证书服务机构签发的证书的订户，包括个人、事业单位、服务器、企业单位、政府机构、社会团体、 网站等提供网上服务和享受网上服务的各种实体，以及其它凡是SZCA各类证书的有效期限未到的订户，均可以请求更新其持有各类证书。

3. 证书更新请求的处理

- 申请者到SZCA 授权的发证机构书面填写“证书更新申请表”。

- SZCA 授权的发证机构遵循第三章识别与鉴定的规则对订户提交的证书更新申请进行查验；
- 发证机构审核通过后，提交申请至SZCA；
- 发证机构为订户制作证书；
- 证书签发后，发证机构将证书产品及其有关资料发给订户。订户接受证书；
- 新证书签发后旧的证书被吊销。

4. 证书更新的注意事项

订户在更新证书前，用户应确保即将到期证书的密钥对的安全可靠。一旦无法确认这种可靠性，SZCA建议订户直接选择证书密钥更新。

5. 构成接受更新证书的行为

在订户在线完成递交更新请求或者离线递交更新请求获得批准后，就意味着申请者已经表示接受了更新证书。SZCA签发证书后将按照订户的更新方式向其发布。

6. 电子认证服务机构对更新证书的发布

一旦订户接受更新证书，SZCA签发后将在其信息库、目录服务中和由SZCA决定的其它一个或多个信息库里发布证书的副本。订户也可以在其它场所公布他们的更新证书。

新证书签发后，旧的证书将被注销。SZCA在目录服务器上发布用户新证书。用户旧证书通过CRL发布。

7. 电子认证服务机构对其它实体的通告

订户接受更新证书后，SZCA将不专门对注册机构、受理点、主管部门等实体进行专门的通告，这些实体可以通过目录服务或者查询SZCA信息库来获得订户的更新证书及相关信息。

6. 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。发证机构默认的方式是为订户选择证书密钥更新。

1. SZCA私有密钥有效期

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。

深圳 CA根私钥的有效期应比其签发的订户证书有效期长。其原因是为了防止电子认证服务机构签发的证书出现刚签发不久即失效的情况。

2. 密钥更新的情形

如出现下列情形的,订户必须选择证书密钥更新：

- 证书到期并且密钥对的试用期也到期
- 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。
- 证书被吊销后需要重新获得证书。

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

证书即将到期的订户，出于安全考虑，应尽量采取证书密钥更新，来获得新的证书。

3. 请求证书密钥更新的实体

所有持有SZCA和其授权的证书服务机构签发的证书的订户，包括个人、事业单位、服务器、企业单位、政府机构、社会团体、 网站等提供网上服务和享受网上服务的各种实体，以及其它凡是SZCA各类证书的有效期限未到的订户，均可以请求证书密钥更新服务。

4. 密钥更新的流程

- 申请者书面填写“证书或密钥更新申请表”；
- SZCA 授权的发证机构遵循第三章识别与鉴定的规则对订户提交的密钥更新申请进行查验；
- 审核通过后，提交申请至SZCA；
- 发证机构为订户更新密钥，产生新的证书并交给订户；
- 新证书签发后，旧的证书将被自动吊销，并通过 CRL 发布。

5. 密钥更新的注意事项

订户在进行密钥更新之前将加密邮件等加密过的文件进行解密，同时备份（例如将邮件内容复制以明文方式存储或将邮件附件保存），然后将证书删除。以上操作完成后才能进行密钥的更新。

如订户未解密文件而进行密钥更新，由此造成的可能损失，SZCA 概不负责。

6. 构成接受密钥更新证书的行为

在订户密钥更新请求获得批准后，就意味着申请者已经表示接受了更新证书。SZCA签发证书后将按照订户的更新方式向其发布。

7. 证书的变更

在证书有效期内，当证书信息发生变化，订户或者其它参与者可选择证书变更，保留原有公钥，申请签发新的证书，SZCA在对申请者提交的资料进行鉴别确认后，将为其重新签发证书。

1. 证书变更的情形

当订户或者其它参与者的信息发生变化，造成实体身份发生变化时，用户必须对原有证书进行变更，或者将证书申请吊销后重新要求签发证书。

2. 请求证书变更的实体

所有持有SZCA发证机构签发的证书订户、包括个人、企业单位、事业单位、政府机构、社会团体、人民团体等各类组织机构等，在信息发生变化、造成实体身份变化时，均可以请求证书变更服务。

3. 证书变更请求的处理

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

4. 变更证书的注意事项

证书修改后，证书的有效期并没有改变，仍然为原证书的有效期。

订户在变更证书前，用户应确保即将该证书的密钥对的安全可靠，一旦无法确认这种可能，那么SZCA建议订户直接选择证书密钥更新。

5. 构成证书变更的行为

在订户完成递交证书变更请求获得批准后，就意味着申请者已经表示接受了变更证书，SZCA签发证书后将按照订户的变更方式向其发布。

6. 电子认证服务机构对变更证书的发布

一旦订户接受变更证书，SZCA签发后将在其信息库、目录服务中发布证书的副本，订户也可以在其它场所公布他们的变更证书。

新证书签发后，旧的证书将被注销，并通过CRL发布。

7. 电子认证服务机构对其它实体的通告

订户接受变更证书后，SZCA将不专门对注册机构、受理点、主管部门等实体进行专门的通告，这些实体可以通过目录服务或者查询SZCA信息库开获得订户变更证书及相关信息。

8. 证书挂起

1. 证书挂起原因

- 证书用户暂停使用证书；
- 其它，例如：订户由于某种原因如长期出差，短期内无法使用证书，可以申请证书挂起。

2. 证书挂起的用户类型

由SZCA 颁发的原有证书有效期限未到的个人、单位、服务器、企业、组织、 网站等提供网上服务和享受网上服务的各种实体，以及其它凡是SZCA 各类证书的有效期限未到的订户。

3. 证书挂起的流程

- 申请者到SZCA 授权的发证机构书面填写“挂起或吊销申请表”， 并注明挂起的原因；
- SZCA 授权的发证机构遵循第三章识别与鉴定的规则对订户提交的证书挂起申请进行查验；

- 强制挂起：SZCA 授权的发证机关管理员可以依法对订户证书进行强制挂起，挂起后必须立即通知该订户。强制挂起的命令来源于：SZCA 或SZCA 授权的发证机构；
- SZCA 挂起订户证书后，发证机构将当面通知或通过各种有效途径（电话、邮件、书面、传真等）通知订户证书已被挂起；
- 订户证书被挂起后，订户必须在证书有效期到期前恢复证书。SZCA将努力通过各种有效途径（电话、邮件、书面文字、传真等）提醒订户，若证书到期订户还是没有回复，SZCA 或SZCA 授权的发证机构有权自行吊销证书。对此造成的任何后果， SZCA 不负任何责任。

4. 证书挂起的注意事项

订户在申请证书挂起时，需在填写“挂起或吊销申请表”时注明原因，并在证书到期前，对进行挂起的证书进行恢复。

9. 证书吊销

1. 证书吊销的原因

- 新的密钥对替代旧的密钥对；
- 密钥失密：与证书中的公钥相对应的私有密钥被泄密或用户怀疑自己的密钥失密；
- 从属关系改变：与密钥相关的订户的主题信息改变，证书中的相关信息有所变更；
- 操作中止：由于证书不再需要用于原来的用途，但密钥并未失密，而要求中止（例如订户离开了某个组织）；
- 证书的更新费用未收到；
- 订户不能履行电子认证业务规则或其它协议、法律及法规所规定的责任和义务；
- 订户申请初始注册时，提供不真实材料；
- 证书已被盗用、冒用、伪造或者篡改；
- 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；
- 其它情况。

2. 证书吊销的用户类型

由SZCA 颁发的原有证书有效期限未到的个人、单位、服务器、企业、组织、 网站等提供网上服务和享受网上服务的各种实体，以及其它凡是SZCA 各类证书的有效期限未到的订户。

3. 证书吊销的流程

- 申请者到SZCA 授权的发证机构书面填写“挂起或吊销申请表”，并注 明吊销的原因；
- SZCA 授权的发证机构遵循第三章识别与鉴定的规则对订户提交的证书吊销申请进行查验；
- 强制吊销：SZCA 授权的发证机构可以对订户的证书进行强制吊销，吊销后必须立即通知该订户。强制吊销的命令来自于：SZCA 或SZCA 授权的发证机构；
- SZCA 吊销订户证书后，发证机构将书面通知订户证书被吊销，并通过CRL向外界公布。

4. CRL 发布频率

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

5. 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吊销。如果黑名单公布证书已经吊销，而依赖方没有查黑名单，由此造成的损失由依赖方本身承担。

6. 证书吊销的注意事项

证书吊销是永久性吊销，不可以进行证书恢复。

- SZCA 没有公开数字证书吊销原因的义务；
- 证书变更、密钥变更后原有证书将被吊销；
- 提交请求时需要注明吊销原因；
- 请订户在进行证书吊销之前将加密邮件等加密过的文件进行解密，同时备份（例如将邮件内容复制以明文方式存储或将邮件附件保存），然后将证书删除。以上操作完成后才能进行证书的吊销。

10. 证书恢复

1. 证书恢复原因

证书被挂起是证书恢复的原因。证书恢复只针对挂起的证书。

2. 证书恢复的用户类型

由SZCA 颁发的原有证书有效期限未到的个人、单位、服务器、企业、组织、 网站等提供网上服务和享受网上服务的各种实体，以及其它凡是SZCA 各类证书的有效期限未到的订户。

3. 证书恢复的流程

- 申请者到SZCA 授权发证机构书面填写“数字证书业务申请表”，勾选“证书恢复”项；
- SZCA 授权的发证机构遵循第三章识别与鉴定的规则对订户提交的证书恢复申请进行查验；
- 发证机构审核通过后，为订户恢复证书。并通知订户证书已被恢复；
- 订户得到恢复通知，证书恢复完成。

11. 密钥恢复

1. 密钥恢复原因

- 加密密钥丢失
- 其它。

2. 密钥恢复的用户类型

由SZCA 颁发的原有证书有效期限未到的个人、单位、服务器、企业、组织、 网站等提供网上服务和享受网上服务的各种实体，以及其它凡是SZCA 各类证书的有效期限未到的订户。

3. 密钥恢复流程

证书订户的加密密钥对是由SZCA代订户向深圳市密钥管理中心申请生成，并由深圳市密钥管理中心进行管理。当订户需要进行加密密钥恢复时，按照深圳市密钥管理中心相关规定、流程，接受

订户的加密密钥恢复申请，为订户进行加密密钥的恢复。

4. 密钥恢复的注意事项

- 密钥恢复只能恢复订户的加密密钥；
- 由于订户丢失签名密钥而造成的后果，SZCA 概不负责。

12. 证书状态查询

SZCA 提供以下两种方式为订户提供证书状态查询服务。

1. CRL

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

2. OCSP

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

13. 服务终止

服务终止是指证书使用者终止与SZCA 的服务，它包含以下两种情况：

- 证书到期时终止与SZCA 的服务；

  当证书到期时，证书使用者不再延长证书使用期或者不再重新申请证书时，证书使用者可以提出服务终止。
- 证书未到期时中止与SZCA 的服务。

  在证书的有效期内，由于证书使用者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挂起或吊销证书。证书使用者与SZCA 的服务终止。

14. 密钥生成、备份与恢复

1. 签名密钥的生成、备份与恢复的策略与行为

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

2. 加密密钥的生成、备份和恢复的策略和行为

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

1. 证书持有人提出申请
2. 国家执法机关、司法机构因执法、司法的需要
3. 国家其它管理部门管理需要
4. 深圳市密钥管理中心批准。

密钥恢复只有在必须的情况下才进行，并且申请要提出充分的理由和提供有关文件、材料。

1. 认证机构设施、管理与操作控制

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。

1. 场地位置与建筑

SZCA认证系统的主机房位于深圳市南山区高新中二路深圳软件园8栋三楼。

机房按照功能分为业务受理区、辅助设备区、服务区、RA管理区、CA管理区、CA核心区、KM管理区、KM核心区。

2. 物理访问

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

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

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，机房室内设计温度：22±1℃，相对湿度：55±5%/h ,同时，机房安置了新风系统，对机房进行换气，保证机房内的空气品质和解决新风供应以及机房对空气清洁度的要求等问题。

4. 水患防治

SZCA的机房位于三楼，认证服务系统所处的环境为密闭式建筑，并且采取相应防水侵蚀措施，充

分保障系统安全。

5. 火灾防护

SZCA 机房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. 介质存储

SZCA对物理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。

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。

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。

8. 异地备份

SZCA对数据进行异地备份，遇到灾难情况发生时保证数据安全。同时，在条件成熟时，建立异地灾备系统。

2. 程序控制

1. 可信角色

SZCA 明确执行 CA 系统的关键职能职位，他们包括但不限于：

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

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

2. 每项任务需要的人数

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

10	审核员	若干
11	制证员	若干

3. 每个角色的识别与鉴别

所有SZCA的在职人员，必须通过认证后，根据作业性质和职位权限的情况，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。

1. 需要职责分割的角色

在SZCA定义的可信角色中，遵循可信角色分离、操作和管理分离的原则，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。

1. 人员控制

1. 资格、经历和无过失要求

SZCA对承担可信角色的工作人员的资格要求如下：

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

1. 背景审查程序

SZCA 员工的录取经过严格的审查，根据岗位需要增加相应可信员工的背景调查。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 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 对其关键的 CA 员工进行严格的背景调查。注册机构、注册分支机构和受理点操作员的审查可以参照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 签定保密协议，合同期满以后 2 年内仍然不得从事与SZCA 相类似的工作。

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

2. 培训要求

SZCA 对SZCA 员工进行以下内容的综合性培训：

- 公司文化及各类管理制度；
- 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。

3. 再培训周期和要求

根据SZCA 策略调整、系统变更等情况，SZCA 将对员工进行继续培训，以适应新的变化。

4. 工作岗位轮换周期和顺序

SZCA认证系统的运行员工和负责认证系统设计、开发的员工承担不同的职责，双方的岗位互相分离，为了保证安全，后者不能成为前者。即开发员工和运行员工分离的原则。
为了配合认证系统的运营需要和岗位适应性的需要，SZCA会选派适当的人选，在不同的岗位进行

轮换。但是这种轮换不得和前面的岗位分离原则相违背。

5. 未授权行为的处罚

当SZCA 员工进行了未授权或越权操作，SZCA 在确认后立即中止该员工进入SZCA认证服务体系。根据情节严重程度，实施包括提交司法机关处理等措施。

一旦发现上述情况，SZCA 立即作废或终止该人员的安全证书和IC卡。

6. 独立合约人的要求

对于不属于SZCA机构内部工作人员，但从事SZCA业务有关工作的如业务分支机构的业务人员、管理人员等独立签约者，SZCA的统一要求如下：

1. 人员档案的备案管理
2. 具有1年以上相关业务工作经验；
3. 接受SZCA一周的岗前培训。

1. 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。

1. 审计日志程序

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。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。

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。

3. 审计日志的保存期限

SZCA 在数据库保存审查记录至少壹个月，离线存档至少七年。

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，严格禁止访问、阅读、修改和删除等操作。

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。

6. 审计收集系统

SCZA 的审计采集系统涉及：

1、 证书管理系统

2、 证书签发系统

3、 证书目录系统

4、 证书审批受理系统

5、 备份恢复系统

6、 其它SZCA认为有必要审查的系统

1. 对异常事件的通告

SZCA 对审查中发现的攻击现象将做详细记录，在法律许可的范围内追溯攻击者，并保留采取相应对策措施的权利，如：切断对攻击者已经开放的服务、递交司法部门处理等措施。

SZCA 有权决定是否通知在审查中发现的攻击者或肇事者。

2. 脆弱性评估

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

1. 记录归档

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。

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。

3. 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能接近它们。SZCA 保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力等的破坏。

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. 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。

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。

7. 获得和检验归档信息的程序

SZCA 每年会验证存档信息的完整性。

2. 电子认证服务机构密钥更替

在这里密钥转换是指当SZCA 根证书到期而需要更换根密钥对时所采取的措施。SZCA 根密钥对由加密机产生。证书到期更换密钥时将签发 3 张证书。

- 使用旧的私有密钥对新的公钥及信息签名生成证书；
- 使用新的私有密钥对旧的公钥及信息签名生成证书；
- 使用新的私有密钥对新的公钥及信息签名生成证书。

通过以上 3 张证书达到密钥更换的目的，使新旧证书之间互相认证、信任。

SZCA 根证书有效期为5年。在SZCA 证书到期之前，SZCA 将对根私有密钥进行更换。密钥转换程序在旧密钥对向新密钥对的转换起着过渡的作用。SZCA 密钥转换采用以下方式：

- SZCA 将在证书到期前的 60 天内停止颁发新的证书；
- 旧的SZCA 证书到期后，SZCA 将用新的 CA 密钥对签发证书。

3. 损害与灾难恢复

灾难恢复情况如下：

SZCA 遭到攻击，造成灾难时的恢复：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 将按照灾难恢复计划实施恢复，具体由SZCA 灾难恢复计划决定；

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将按照灾难恢复计划实施恢复。

2. 计算资源、软件和/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的系统备份与恢复方案，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。

3. 实体私钥损害处理程序

SZCA的根私钥出现损毁、遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时：

1. 立即向电子认证服务管理办公室和其它政府主管部门汇报，并立即吊销所有已经被签发的证书，更新CRL和OCSP信息，供证书订户和依赖方查询。同时SZCA立即生成新的密钥对，并自签发新的根证书。
2. 新的根证书签发以后，按照本CPS关于证书签发的规定，重新签发下级证书和SZCA下级操作子CA证书。
3. SZCA新的根证书签发以后，将会立即通过SZCA信息库、目录服务器、HTTP等方式进行发布。

SZCA下级操作子CA证书的私钥出现遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时：

1. 立即向SZCA进行汇报并生成新的密钥对和证书请求，向SZCA申请签发新的证书。
2. 立即吊销所有已经被签发的证书，更新CRL和OCSP信息，供证书订户和依赖方查询。
3. 新的根证书签发以后，按照本CPS关于证书签发的规定，重新签发订户证书。
4. 新的证书签发以后，将会立即通过SZCA信息库、目录服务器、HTTP等方式进行发布。

证书订户的私钥出现遗失、泄露、破解、被篡改，或者有被第三者窃用的疑虑时，订户应该按照本CPS的规定，首先申请证书吊销，并按照规定重新申请新的证书。

1. 灾难后的业务连续性能力

SZCA在遭遇本节5.7.1和5.7.2中描述的灾难后，通过其备份机制，将尽快恢复各项业务的正常运行。

1. 电子认证服务机构或注册机构的终止

当SZCA 打算终止经营时，会在终止经营九十日前给SZCA 授权的发证机构、订户以及其他相关各方书面通知，并在终止服务六十日前向信息产业主管部门报告,按照相关法律规定的步骤进行操作。

在终止期间，采用以下措施终止业务：

- 起草 CA 终止规则；

- 通知与 CA 停止相关的实体；
- 关闭从目录服务器；
- 证书吊销；
- 处理存档文件记录；
- 停止认证中心的服务；
- 存档主目录服务器；
- 关闭主目录服务器；
- 管理SZCA 系统管理员和SZCA 安全官员；
- 处理加密密钥；
- 处理和存储敏感文档；
- 清除 CA 主机硬件。

1. 认证系统技术安全控制

1. 密钥对的生成和安装

由于密钥对是安全机制的关键，所以在《SZCA电子认证业务规则》中制定了相应的规定，确保密钥对的产生、传送、安装等具备保密性、完整性和不可否认性。

1. 密钥对的生成

- 加密密钥对：加密密钥对是由中华人民共和国国家密码管理局（以下简称国家密码管理局）许可的、SZCA 数字证书签发系统支持的加密机设备生成的，由深圳市国家密码管理委员会办公室所属的KMC 控制管理。
- 签名密钥对：签名密钥对由用户端产生，证书申请者可使用深圳市国家密码管理委员会办公室认可的、SZCA 数字证书签发系统支持的介质生成签名密钥对。签名密钥存储在介质中不可导出，保证SZCA 无法复制签名密钥对。

2. 私钥传送给订户

证书用户的加密私钥在 KMC 产生，该私钥只保存在 KMC。在加密私有密钥从 KMC 到用户的传递过程中采用国家密码管理局许可的对称密钥算法加密。用户使用自己的证书载体解密该私钥,保证了证书用户的密钥安全。

3. 公钥传送给证书签发机构

SZCA 从 KMC 取得用户公钥后为其签发证书，在此过程中也采用国家密码管理局许可的对称密钥算法加密，保证传输中数据的安全。

4. 电子认证服务机构公钥传送给依赖方

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

5. 密钥的长度

SZCA 所使用的密钥对长度支持 1024 位。

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. 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。

2. 私钥保护和密码模块工程控制

1. 密码模块的标准和控制

SZCA 使用国家密码管理局许可的产品，密码模块的标准符合国家规定的要求。

2. 私钥多人控制

SZCA 采用多人控制策略激活、使用、停止SZCA 的签名密钥。

3. 私钥恢复

密钥管理中心的密钥采用密钥恢复机制，对密钥管理中心生成的加密密钥对由密钥管理中心管理，确保国家对任何使用密钥加密的数据都能依照法律流程进行司法恢复。

4. 私钥备份

证书的持有者可以备份他们的私有密钥，以确保这些私有密钥的安全。KMC 备份托管的加密私有密钥，确保加密私有密钥的安全。

5. 私钥归档

KMC 提供过期的托管私有密钥的存档服务。

6. 私钥导入、导出密码模块

在SZCA 证书服务体系中，使用SZCA 的软件可以把私有密钥导入密码模块中。

私有密钥无法从硬件及软件密码模块中导出。必须通过密码验证之后，才可能使用存储在密码模块中的私有密钥进行加解密操作。

7. 私钥在密码模块的存储

证书的持有者可以将私有密钥保存在硬件密码模块中，也可以保存在软件密码模块中。SZCA的签名私有密钥必须保存在硬件密码模块中。

8. 销毁私钥的方法

凡用户需要销毁私有密钥，应通知SZCA，由 KMC 进行销毁。

9. 密码模块的评估

SZCA使用国家密码主管部门批准和许可的密码产品，接受其颁布的各类标准、规范、评估结果、评价证书等各类要求。

3. 密钥对管理的其它方面

1. 公钥归档

公钥的归档，其操作过程、安全措施、保存期限以及保存策略和证书保持一致。

2. 证书操作期和密钥对使用期限

公钥、私钥的有效期相同，并且和SZCA签发的证书的有效期相同。

4. 激活数据

1. 激活数据的产生和安装

敏感数据包括SZCA 提供的证书私有密钥口令、被加密的数据等。SZCA 提供唯一的不可猜测的证书私有密钥口令。这些私有密钥口令由SZCA 根据授权和操作的许可实施批准并且仅发放给授权用户。

2. 激活数据的保护

SZCA 采取加解密机制等多种方式保护敏感数据，以避免未授权的使用。未授权用户企图使用敏感数据达到预定的数目时，敏感数据会自动锁定。

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

1. 计算机安全控制

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。

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。

2. 生命周期技术控制

1. 系统开发控制

SZCA 的软件设计和开发过程遵循以下原则：

- 第三方的验证和审核
- 安全风险和可靠性设计

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。

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。

3. 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。

1. 证书、证书吊销列表和在线证书状态协议

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。

1. 版本号

SZCA签发的证书符合X.509 V3 版证书格式。

2. 证书扩展项

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

1、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。即SZCA各个属性，包括国家、省、市、组织机构、单位部门、和通用名。
- CN=SZCA=ShenZhen Digital Certificate Authority Center CO.LTD
- 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。
- 证书主题（Subject）：指定证书持有者的X.500唯一名字。包括国家、省、市、组织机构、单位部门和通用名，还可包含E-mail地址等个人信息等。
- 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。

2、证书扩展项

- 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时，用来唯一标识签发者的X.500名字。
- 主题密钥标识符（Subject Unique Identifier）：此域用在当同一个X.500名字用于多个证书持有者时，用来唯一标识证书持有者的X.500名字。
- 密钥使用：指定各种密钥的用法：电子签名，不可抵赖，密钥加密，数据加密，密钥协议，验证证书签名，验证CRL签名，只加密，只解密，只签名。
- CRL 发布点：由SZCA 定义的 CRL 发布点。

3、自定义扩展项

针对不同的证书应用服务SZCA自定义了一些扩展项

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

3. 算法对象标识符

SZCA签发的证书中，密码算法的标识符为sha1RSA。

4. 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。

5. 名称限制

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

2. CRL（证书吊销列表）

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

1. CRL版本

SZCA的证书吊销列表采用X.509 v2 版的证书格式。

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 sha1RSA 签名算法。
- 颁发机构密钥标识符（Issuer Unique Identifier）：此域用在当同一个X.500名字用于多个认证机构时，用来唯一标识签发者的X.500名字。
- 吊销证书列表：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—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。

3. CRL下载

SZCA证书用户可以通过SZCA网站http://www.szca.gov.cn/下载CRL。

3. OCSP（在线证书状态查询服务）

SZCA 为证书用户提供 OCSP（在线证书状态查询服务），OCSP 为 CRL 的有效补充，方便证书用户及时查询证书状态信息。SZCA OCSP 服务遵循 RFC2560 标准。

1. OCSP请求

一个OCSP状态请求包括以下域：

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

2. OCSP响应

当一个确定的OCSP的响应消息包含以下域：

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

3. OCSP定义的扩展项

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

2. 认证机构审计与评估

1. 审计的频率与情形

为了检查、确认SZCA作为第三方认证机构是否按照其CPS、业务规范、管理制度和安全策略开展业务，同时发现机构运营过程中存在的可能风险，SZCA将依照严格的审计方法和审计过程对CA中心及其注册机构进行定期审计，以评估这些机构是否符合SZCA的CPS以及相关的规范、操作程序和标准。

2. 审计者的身份与资质

1. SZCA 的内部审计

内部审计组织为SZCA 运营安全管理小组。SZCA 运营安全管理小组定期按照严格的审计方法和审计过程，对CA中心及其注册机构进行审计，评估其是否符合本CPS以及相关的规范、操作程序和标准。

2. SZCA 的外部审计

SZCA无条件接受信息产业主管部门的评估。

SZCA的外部审计，包括信息产业部电子认证服务管理办公室一年一度的审计。

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。

3. 评估者与被评估者之间的关系

外部评估者(信息产业主管部门或者其委托的其它机构)和SZCA之间是独立的关系，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。

SZCA可以根据需要，选择专业、公正、客观的专业审计评估机构，协助进行内部评估。

4. 评估内容

对SZCA 规范审计包括：

- 是否制订和公告CPS及相关的操作规范。
- SZCA 支持的证书认证操作规程是否与本电子认证业务规则表达一致。
- 是否按照CPS来制订相关的操作规范和运作协议
- 是否按照CPS相关操作规范和运作协议开展证书申请注册等服务
- SZCA 是否实施了相关技术、管理、相关政策和业务规则。
- 服务的完整性：密钥和证书生命周期的安全管理、证书吊销和挂起的操作、业务系统的安全操作、业务操作标准审查。
- 物理和环境安全控制：信息安全管理、人员的安全控制、建筑设施的安全控制、软硬件设备和存储介质的安全控制、系统和网络的安全控制、系统开发和维护的安全控制、灾难恢复和备份系统的管理、审计和归档的安全管理等。
- 审计者或SZCA 认为有必要审计的其它方面。

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运营安全管理小组和被评估者，进行后续处理。

SZCA 将根据普遍认可的国际惯例或 监管法律迅速解决问题。

6. 评估结果的传达与发布

信息产业主管机构在完成评估后，按照法律法规的要求对评估结果进行处理。

SZCA的内部评估结果在与被评估对象的相关人员进行讨论确定后，将其视为机密资料进行处理，只有被评估对象和评估人员以及SZCA运营安全管理小组可以了解。非经SZCA运营安全管理小组的批准或者被评估对象的授权，评估人员不泄露给任何其它无关的第三方知晓。

在必要的情况下，对SZCA关联单位（包括RA、LRA以及其它SZCA授权的证书服务机构或其它形式的关联体）通知审计结果的详情和具体方法，将在SZCA和另一方的独立协议中写明。

任何第三方向SZCA关联单位通知审计结果或者类似的信息，都必须事先明确的向SZCA表明通知的目的和方式，并征得SZCA的同意，法律另有规定的除外；SZCA保留在这方面的法律权力。

3. 法律责任和其它业务条款

1. 费用

SZCA 对订户和所有使用SZCA证书的各方（SZCA 体系的关联单位包括SZCA 注册机构、注册分支机构、证书制作受理点等）收取服务费用。订户和SZCA 关联单位有义务根据SZCA 的价目表支付给SZCA 费用。

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

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

1. 证书签发和更新费用

SZCA对证书签发和更新的费用，公布在SZCA的网站http：//www.szca.gov.cn上，供用户查询。
该公布价格参照广东省物价局《电子认证服务收费项目和收费标准》执行。

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。

2. 证书查询费用

对于证书查询，目前SZCA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。

如果该项证书查询的收费政策有任何变化，SZCA将及时在网站http：//www.szca.gov.cn上予以公布。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。

3. 证书吊销或状态信息的查询费用

对于证书吊销或状态信息的查询，目前SZCA暂不收取任何费用。如果该项证书查询的收费政策有任何变化，SZCA将会及时在网站http：//www.szca.gov.cn上予以公布。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。

4. 其它服务费用

其它相关服务费用，SZCA将公布在SZCA的网站www.szca.gov.cn上，供用户查询。

5. 退款策略

SZCA对用户收取的费用中，除了证书申请和更新费用外，包括但不限于证书查询费用、证书吊销和状态查询费用等。

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。如果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，订户可以要求SZCA吊销证书并退款。在SZCA吊销了订户的证书后，SZCA将立即把订户为该证书所支付的全额费用退还给订户。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。

2. 财务责任

SZCA每年定期委托公正、客观的第三方进行财务审核。

1. 保险范围

SZCA根据业务发展情况决定其投保策略，目前暂无。

3. 商业信息的保密

1. 保密的商业信息范围

SZCA与SZCA授权的发证机关之间、SZCA与订户之间、SZCA 授权的发证机构与订户之间、SZCA与其它证书服务相关方、SZCA关联体之间的协议、往来函和商务协定等，除非法律明确规定，不能在未经另一方许可的前提下擅自公开。

与证书持有者证书公钥配对的私钥，证书持有者应该遵照本CPS的规定认真保管，不能公布给未经授权的任意第三方，如果证书持有者擅自泄露私钥，则由此引起的后果由证书持有者自负。
SZCA或SZCA对发证机构的审计报告、审计结果等相关信息是保密信息， 除了SZCA 授权和信任的员工，不能泄露给其它任何人。这些信息除了用于审查目的或法律规定的目的外，不能用于其它用途。

有关SZCA认证体系的运营信息只能在严格的指定情况下，才能传授给SZCA授权的员工，这种传授并不意味着对信息公开的授权。对SZCA来讲，所有涉及系统运营的信息，都在保密范围之内。除非法律明文规定，SZCA 没有义务公布或透露订户证书以外信息。同时，SZCA在与其它SZCA授权的证书服务机构或其它形式的关联体签署授权协议时，都将此作为必须满足的要求。

2. 非保密的商业信息

与证书有关的申请流程、申请需要的手续、申请操作指南、CPS等信息是可以公开的。而且SZCA在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。
非保机密信息还包括证书持有者证书中包括的相关信息。证书中的持有者信息是可以公开的，通过SZCA目录服务等方式向外公布。

SZCA 在目录服务器中公布证书的作废信息，供网上查询。

这些非保密信息，并不能够被任意不被授权的第三方使用，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。

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，都有义务按照本CPS的规定，承担相应的保护保密信息的责任。

当SZCA 在任何法律、法规或规章条款的要求下，或在法院的要求下必须披露本电子认证业务规则中具有保密性质的信息时，SZCA 可以按照法律、法规或规章条款以及法院的判定的要求，向执法部门公布相关的保密信息。这种披露不视为违反了保密的要求和义务。

当机密信息的所有者出于某种原因，要求SZCA公开或披露他所拥有的保密信息，SZCA应满足其要求；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。

4. 个人信息的保密

1. 隐私保密方案

SZCA尊重所有的用户和他们的隐私，并按照法律法规的要求和国际公认的个人数据隐私保护原则执行，如果有与此相关的明确的隐私保护法律（如个人信息保护法）的出台，那么本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。

关于SZCA的隐私条款规则，包括如下：

- 信息的分类处理
- 信息使用
- 信息披露

SZCA保留在不预先通知的情况下随时修改个人隐私保密条款的权利。目前的隐私保密条款是有效的。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。

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。

下列信息将被作为隐私处理，需要采取可靠、严格的保密措施予以保护：

- 订户的有效证件号码，如身份证号码，护照号码，单位组织机构代码等。
- 订户的联系电话；
- 订户的通信地址和住址；
- 订户的银行帐号；
- 订户提交的身份证明文件上包含的隐秘性信息等。

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。

SZCA定义包括但不限于以下信息不被视为证书订户的隐私信息：

- 订户的姓名、单位名称等；
- 订户的性别、单位性质等；
- 订户的通信地址的邮政编码；
- 订户的电子邮箱。

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在任何法律法规或者法院通过合法程序的要求下，或者信息所有者书面授权的情况下，SZCA可以向特定对象公布相关的隐私信息。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。

5. 使用隐私信息的告知与同意

SZCA在其认证业务范围内使用所获得的任何订户信息，只用于订户身份识别、管理、和服务订户的目的。在使用这些信息时，无论是否涉及到隐私，SZCA都没有告知订户的义务，也无需得到订户的同意。

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

6. 依法律或行政程序的信息披露

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

- 政府法律法规的规定并且经过主管单位合法的授权程序提出申请
- 法院处理因使用证书产生的纠纷或仲裁时合法的提出申请
- 具有合法司法管辖权的诉讼、仲裁机构的正式申请
- 证书订户以书面方式进行授权

7. 其它信息披露情形

证书订户以书面方式进行授权，要求SZCA向特定对象提供隐私信息时，SZCA可以将信息提供给该订户指定的接受对象；非经订户本人的书面授权，SZCA将拒绝任何第三者的披露请求。

除了法律法规和主管部门的合法请求，以及信息所有人的书面授权，或者SZCA的合法用途以外，SZCA目前不存在任何其它的隐私信息披露情形。

5. 知识产权

SZCA 享有并保留对证书以及SZCA 提供的全部软件的独一无二的一切知识产权，包括保证证书和软件的完整权、名称权和利益分享权等。因此，SZCA 有权决定关联机构采用什么软件系统，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。

按本电子认证业务规则的规定，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。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。

6. 陈述与担保

除非SZCA在协议中作出特别约定，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。

1. 电子认证服务机构的陈述与担保

SZCA的一般陈述：

- 建立电子认证业务规则（CPS）和其它认证服务所必需的规范、制度体系。
- 在本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。
- 除非已通过发出了SZCA的私钥被破坏或被盗的通知，保证SZCA本身的签名私钥得到安全的存放和保护，SZCA 建立和执行的安全机制符合国家相关政策的规定。
- 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，作出与上述规定相反的陈述。

SZCA对订户的陈述。

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，及时吊销或挂起证书。
- 发证机构将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，既视为发证机构作出了上述描述的合理的努力。

发证机构对依赖方的陈述。

发证机构就其所发证书向所有按照本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。

SZCA有关公开发布的陈述

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

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，并依据授权设置和管理各类下级证书服务受理机构，包括RA、LRA等。
- RA必须遵循SZCA制订的服务受理规范、系统运作规范和管理规范，根据本CPS、SZCA公布的规范，RA有权决定是否给申请者提供相应的证书服务。
- 按照SZCA的要求和规范，确定下属证书服务受理机构的设置方式、管理方式和审核方式，这些方式的确定必须以书面的文件形式公布，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必须能够提供证书服务全部的数据资料及备份，并按照SZCA的要求，保证其与下属证书服务机构间的信息传输安全。重要的是，RA承诺严格执行为所有证书用户提供资料的义务，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。
- 接受SZCA对所有证书服务申请者的服务请求拥有最终处理权。
- 不得拒绝任何来自SZCA的公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。
- 为用户提供必要的技术咨询，使用户顺利地申请和使用证书。

3. 订户的陈述与担保

一旦接受发证机构签发的证书，从接受之时起直至证书的整个使用有效期内，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作出如下保证：

- 在证书申请表上填列的所有声明和信息必须是完整、精确、真实和正确的，可供SZCA检查和核实；并且，愿意承担任何提供虚假、伪造等信息的法律责任
- 如果存在代理人，那么订户和代理人两者负有联带责任。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
- 用与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、挂起或吊销）。
- 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。
- 订户是最终订户而不是发证机构。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）所从事的功能，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）或证书吊销列表。
- 一经接受证书，既表示订户知悉和接受本CPS 中的所有条款和条件，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：既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。
- 不得拒绝任何来自SZCA的公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

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。

- 信任体在信赖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作废时，SZCA才保证该证书是有效的；检查该证书证书链中所有出现过的证书的可靠性；检查过该证书的有效期。
- 一旦由于疏忽或者其它原因违背了合理检查的条款，依赖方愿意就而此给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。
- 不得拒绝任何来自SZCA的公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

5. 其它参与者的陈述与担保

垫付商的陈述：

- 垫付商必须承担其所有垫付的证书费用，并按SZCA规定的方式付清。
- 垫付商的垫付行为，就表明其愿意并且能够承担本CPS规定的，对证书服务申请者的身份真实性提供担保的责任。
- 不得拒绝任何来自SZCA的公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

7. 担保免责

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

1. 不保证证书订户、信赖方、其它参与者的陈述内容；
2. 订户违反本CPS § 9.6.3之承诺时，或者证书依赖方违反本CPS § 9.6.4之承诺时，得以免除SZCA的责任；
3. 不对电子认证活动中使用的任何软件作出保证。

1. 有限责任

根据中华人民共和国公司法、中华人民共和国电子签名法和其它法律法规的规定，作为依法设立的有限责任公司，SZCA在承担任何责任和义务时，只承担法律范围内的有限责任。

在本CPS 和SZCA与任何一方签订的协议中，SZCA不做任何其它保证和履行任何进一步的义务。

2. 赔偿

1. 赔偿范围

在认证活动中产生的赔偿，都以本CPS的规定为处理依据，法律法规或政府主管机构另有要求的除外。SZCA赔偿责任：

- 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；
- 证书订户或者其它有权提出吊销或挂起证书的人提出吊销或挂起请求后，到SZCA实际完成吊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。
- SZCA所有的赔偿义务不得高于§9.9.2规定的上限；
- SZCA只在SZCA证书有效期内承担损失赔偿责任。

订户赔偿责任：

- 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，订户应赔偿一切损害责任；
- 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、第三者遭受损害的，订户应承担一切损害赔偿责任。
- 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，订户或者依赖方应自行承担一切损害赔偿责任。
- 用户使用或信赖证书时，未能依照本CPS等规范进行合理审核，导致SZCA或第三方遭受损害的，应由该用户担负一切损害赔偿责任。
- 证书订户或者其它有权提出吊销或挂起证书的人提出吊销或挂起请求后，到SZCA实际完成吊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，参照其规定。

2. 赔偿限额

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、挂起或吊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。

1. 有效期和终止

1. 有效期限

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

2. 终止

本CPS及其更新版本在SZCA终止电子认证服务时失效。

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。

对本CPS终止之日前发生的法律事实，CPS中各方责任的规定及免责仍然适用。

2. 对参与者的个别通告与沟通

本CPS终止后，SZCA对文档失效的有关事项，应通知参与本机构电子认证活动的各项有关当事人。

3. 修订

SZCA有权修订SZCA CPS并有权把修订结果以CPS修订版的形式通过网站www.szca.gov.cn发布，或者放在SZCA信息库里。

1. 修订程序

SZCA将尽量避免《SZCA电子认证业务规则》进行不必要的修改。但SZCA将不定期地对《SZCA电子认证业务规则》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。

当SZCA认为有必要对《SZCA电子认证业务规则》进行修改时，SZCA运营安全管理小组将对《SZCA电子认证业务规则》及其它相关的文档、协议提出修改建议，获得SZCA管理层及运营安全管理小组负责人同意后，运营安全管理小组将负责组织对《SZCA电子认证业务规则》及其它相关的文档、协议的修改。修改后的《SZCA电子认证业务规则》及其它相关的文档、协议，经SZCA管理层及运营安全管理小组批准后正式发布。并自公布之日起三十日内向信息产业部备案。

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 www.szca.gov.cn 信息库中设置和公布修订结果。如果关于SZCA CPS 的修改被放置在SZCA信息库中的规范更新和通知栏(查看www.szca.gov.cn)，它对于修改SZCA CPS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。

3. 修订同意

如果在修订的CPS发布后的15 天内，证书申请者和订户没有请求吊销其证书的话，就被认为同意该修订，所有的修订和改变立刻生效。

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：

- 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

对CPS 的必要修订将在发布15天以后生效。 除非在这15天结束前，SZCA以同样的方式发表一个撤消修订的通知。

对CPS 的非必要修改在发布之日起立即生效。SZCA 能够自由决定哪个修改是非必要修改。

4. 争议处理

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

如果争议中的当事人书面一致同意选择争议解决机制（比如仲裁），否则就执行SZCA CPS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。

5. 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，SZCA CPS 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。

6. 与适用的法律的符合性

所有电子认证活动的参与方，都必须遵守《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》以及其它中华人民共和国法律法规的规定。

7. 一般条款

1. 完整协议

SZCA CPS中直接影响SZCA的权利和义务的条款和规定，除非通过受到影响的当事人向SZCA发出信息或文件，要求对SZCA CPS中SZCA的权利和义务的条款和规定进行修正、放弃、补充、修改或终止，且得到SZCA的同意,或者另有其它规定，否则不能进行口头上或单方面的修正、放弃、补充、修改或终止。

在SZCA CPS和其它规则、方针或协议发生冲突时，所有认证活动的参与方都将受SZCA CPS规定的约束，但以下所示协议除外：

- 在CPS 的发表日期以前签定
- 该合同明确表示替代CPS 处理相关各方事务，或SZCA CPS的规定被法律禁止执行。

2. 转让

无论是各方明示的或暗示的转让人和受让人，SZCA CPS均保证其权益，并对其有约束力。各方可根据法律转让SZCA CPS 详述的权利和义务。

转让操作的终止或暂停根据本CPS的规定进行，或着该转让在转让发生时不影响到转让方对另一方的任何债务或责任的更新。

3. 分割性

SZCA CPS的任何条款或其应用，如果因为任何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，SZCA CPS所规定的责任限制、保证或其它免责条款或限制、或损害赔偿的排除等，均可独立于其它条款的个别条款，并可加以执行。

4. 强制执行

无论出于何种原因，一方未执行SZCA CPS 的某项规定，不被认为是其将来不执行该项或其它规定。

5. 不可抗力

SZCA将不对以下超越其控制能力的不可抗力事件，所造成SZCA CPS规定的担保责任的违反、延误或无法履行负责：构成不可抗力的事件包括战争、恐怖袭击、罢工、瘟疫、自然灾害、火灾、地震、供应商或卖方执行失败、因特网或其它基础设施的瘫痪和其它天灾等等。

8. 声明

SZCA根据《**SZCA电子认证业务规则修订规范**》，有权对本CPS进行修改。

9. 其它条款

SZCA对本CPS具有最终解释权。

10. 补充说明