粤港互认电子认证业务规则

——深圳市电子商务安全证书管理有限公司

版本：V1.0

版本控制表

版本	修改状态	修改说明	审核/批转	生效日期
V0.8	起草	根据粤港互认策略起草	安全策略管理委员会	2018 年 4 月 26 日
V1.0	修订	机构身份鉴别章节精简，修改信息使用授权内容	安全策略管理委员会	2021 年 12 月 29 日

目　录

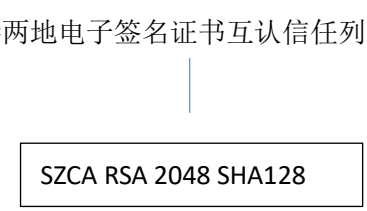
1. 概括性描述

1.1 概述

深圳市电子商务安全证书管理有限公司（以下简称“深圳 CA”或“SZCA”），成立于 2000 年 8 月，通过中华人民共和国工业和信息化部与国家密码管理局资格审查获得《电子认证服务许可证》与《电子认证服务使用密码许可证》，是中国大陆境内合法的第三方电子认证服务机构。

粤港互认电子认证业务规则（以下简称：本 CPS， Certification Practice Statement）是关于认证机构（CA，Certification Authority）在《粤港两地电子签名证书互认办法》和《粤港电子签名证书互认证书策略》的框架下 SZCA 面向中华人民共和国内地自然人、法人、非法人组织电子签名证书（以下简称证书）服务生命周期（如签发、吊销、更新）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 是 SZCA 粤港互认体系下的业务规则。

粤港互认体系结构如下：



SZCA 的所有 CA，包含子 CA 均由 SZCA 所有，由 SZCA 完全直接控制。

本 CPS 的编制遵从 IETF RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,公钥基础设施证书策略和证书运行框架)、《中华人民共和国电子签名法》、国家密码管理局颁布的《证书认证系统密码及相关安全技术规范》、《电子认证服务密码管理办法》、 中华人民共和国工业和信息化部颁布的《电子认证服务管理办法》、《电子认证业务规则规范（试行）》，以及由粤港两地的

① “信任列表”广东省经济和信息化委员会发布地址：http://www.gdei.gov.cn/wzgn/list/201706/t20170628_126655

政府部门[②]共同成立粤港电子签名证书互认试点工作组发布的《粤港两地电子签名证书互认办法》和《粤港电子签名证书互认证书策略》。

SZCA 获得了主管单位中华人民共和国工业和信息化部颁发的电子认证服务许可等资质，并处于资质有效期内；且通过广东省经济和信息化委员会粤港互认资质审查，并经工信部核准，获得粤港电子签名证书认证资质，于 2016 年 11 月加入粤港两地电子签名证书互认信任列表。

1.2 文档名称与对象标识

本文档的全称是《深圳市电子商务安全证书管理有限公司粤港互认电子认证业务规则》，简称为《深圳 CA 粤港互认 CPS》、《SZCA 粤港互认 CPS》或本 CPS，《深圳 CA 粤港互认电子认证业务规则》等同样是指称本文档。本文档，针对的是深圳 CA 签发的粤港互认证书，是对粤港互认证书的管理操作规范的详细描述，及有关认证参与主体的法律责任的重要说明。

SZCA 根据《粤港电子签名证书互认证书策略》中工信部的对象标识（OID）如下：

自然人：2.16.156.339.1.1.1.2.2

法　人：2.16.156.339.1.1.2.2.2

1.3 电子认证活动的参与者

本 CPS 所指的电子认证活动参与者，具体包括电子认证服务机构、注册机构、订户、依赖方及其他参与者，既包括电子认证法律关系中的电子认证服务机构、注册机构、订户及其他参与者，也可能涵盖电子证书应用法律关系中的电子认证服务机构、订户、依赖方及其他参与者。下面就以上主体分别进行描述。

[②]具体指中华人民共和国工业与信息化部、广东省经济和信息化委员会和香港特别行政区政府资讯科技总监办公室。

1.3.1 电子认证服务机构

电子认证服务机构 CA（Certification Authority）承担证书签发、更新、吊销、密钥管理、证书查询、证书黑名单（又称证书吊销列表或 CRL）发布、政策制定等工作。

1.3.2 注册机构

注册机构 RA(Registration Authority)负责订户证书的申请受理、审批和管理，直接面向证书订户，并负责在订户和 CA 之间传递证书管理信息。

深圳 CA 的注册机构是经深圳 CA 授权的证书申请处理机构，是连接和沟通证书申请者和深圳 CA 的桥梁，直接面向的是证书申请者。RA 一般分为两种类型，一种是深圳 CA 设立的机构内部的业务分支机构或者职能辅助部门，隶属于深圳 CA 并直接受深圳 CA 管理；另一种则是与深圳 CA 合作通过相关协议承担深圳 CA 的 RA 职能的第三方机构，此类 RA 受深圳 CA 的委托授权阶段性地成为 RA。其要在授权范围内开展认证业务，并且如果超越授权范围，或者违反约定的范围和要求，违约处理证书申请造成深圳 CA 损失的，要承担相应的损失赔偿责任及其他法律责任。

但二者在受理深圳 CA 的证书业务时，都需要遵照本 CPS 和相关法律法规，合法开展各种证书申请的受理、身份审核、证书发放，证书申请的处理等业务。

1.3.3 订户

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

1.3.4 依赖方

依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的实体。

1.3.5 其他参与者

除电子认证服务机构（SZCA）、订户和依赖方以外的参与者称为其它参与者。

1.3.6 受益者及责任

SZCA 粤港互认下的证书相关联的参与者均为受益者。

1.3.6.1 受益方

SZCA 粤港互认下的证书可以为下述机构提供信赖保证：

（1）所有提交订户协议的订户

（2）获取证书的申请者

（3）获取证书的软件供应商

（4）证书在生效期间的信赖方

1.3.6.2 粤港互认下的证书可提供的保证

（1）证书拥有者的合法存在性

（2）证书拥有者的身份经过有效识别

（3）证书拥有者通过 CA 核实,证书中所有内容均经过验证

（4）证书中关于证书拥有者信息的准确性

（5）提交订户协议

（6）证书状态 7*24 小时可查询

（7）CA 根据本 CPS 规则，废止不符合生效条件的证书

1.4 证书应用

1.4.1 证书类型及适合的证书应用

本 CPS 主要适用于粤港跨境电子交易使用的自然人电子签名证书和法人电子签名证书（以下简称为“个人证书”和“机构证书”，或统称为“粤港证书”）。本 CPS 亦适用于签发上述证书的 SZCA 本身的证书（以下简称为“电子认证服务机构本身的证书”）。

1.4.1.1 个人证书

用于区分、标识、鉴别自然人身份的应用场合。

可用于自然人身份识别以及在应用过程中进行电子签名活动，以实现信息保密性、完整性和不可抵赖性。

1.4.1.2 机构证书

用于区分、标识、鉴别法人、非法人组织身份的应用场合。

可用于法人、非法人组织身份识别以及在应用过程中进行电子签名活动，以实现信息保密性、完整性和不可抵赖性。

1.4.2 限制及禁止的证书应用

SZCA 签发的粤港互认证书，在中国内地法定禁止的应用范围如下：

涉及婚姻、收养、继承等人身关系的；

涉及土地、房屋等不动产权益转让的 ；

涉及停止供水、供热、供气、供电等公用事业服务的；

法律、行政法规规定的不适用电子文书的其他情形。

SZCA 签发的粤港互认证书，在香港法定的证书禁止应用的范围如下：

遗嘱、遗嘱更改附件或任何其他遗嘱性质的文书的订立、签立、更改、撤销、恢复效力或更正。

信托(归复信托、默示信托及法律构定信托除外)的订立、签立、更改或撤销。

授权书的订立、签立、更改或撤销。

订立、签立或订立及签立根据《印花税条例》(第 117 章)须加盖印花或加以签注的文书，该条例第 5A 条所指的协议所关乎的成交单据除外。

政府的批地协议及条件及政府租契。

《土地注册条例》(第 128 章)提述的会影响香港的任何一幅地、物业单位或处所的契据、转易契、其他书面形式的文件或文书、判决及待决案件。

《物业转易及财产条例》(第 219 章)所指的任何转让、转让契、按揭或法定押记，任何其他关乎不动产或不动产权益的处置的合约，或任何其他达成该等处置的合约。

《土地注册条例》(第 128 章)第 2A 条提述的达成浮动押记的文件。

誓言及誓章。

法定声明。

法院判决(包括第 6 条提述的判决)或法院命令。

法院或裁判官发出的手令。

可流转票据(但不包括注有“not negotiable”字样的支票)。

（2）SZCA 与订户约定的证书禁止应用范围。

（3）证书禁止在任何违反国家法律、法规的情形下使用，否则由此造成的法律后果由订户自行承担。

1.5 策略管理

1.5.1 策略文档管理机构

SZCA 指定“SZCA-CPS 策略发展小组”负责 CPS 的起草、注册、维护和更新。本 CPS 的版权完全归属 SZCA 所有。

“SZCA-CPS 策略发展小组”由公司法务人员和技术人员组成，负责本 CPS 的日常管理及维护工作，包括一般性修订及有关本 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。

1.5.2 联系方式

如有需要，请联络：

部门：深圳市电子商务安全证书管理有限公司 SZCA-CPS 策略发展小组

电话：0755-26588399

传真：0755-8615 6366

电子邮件：cps@szca.com

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

1.5.3 决定 CPS 符合策略的机构

“SZCA 运营安全管理小组”是决定 SZCA 电子认证服务所有策略符合性的最高决策机构。其由 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 及其他补充文件或附属于本 CPS 的文件的符合性，及修订、升版的核准与驳回。

1.5.4 CPS 批准程序

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

“SZCA-CPS 策略发展小组”负责将 CPS 定稿提交“SZCA 运营安全管理小组”审阅。经该小组审议通过后，方可对外发布 CPS。发布方式应符合行业标准和通行做法，发布方式包括但不限于网上公布和向客户或合作对象书面提交。发布工作由“SZCA-CPS 策略发展小组”协调相关部门完成，并将“SZCA 运营安全管理小组”审批意见及 CPS 电子版存档。

自发布之日起，对各种主体通过各种方式提供的 CPS 必须与网站上 CPS 保持一致，“SZCA-CPS 策略发展小组”在 CPS 公布之日起三十日内依法将此 CPS 向中华人民共和国工业和信息化部及粤港电子签名证书互认试点工作组备案。

1.6 定义和缩写

表 1.1-定义与缩写

缩写/名词	定义
SZCA	深圳市电子商务安全证书管理有限公司的缩写

SZCA 网站	http://www.szca.com
电子认证服务机构	(Certificate Authority, CA)SZCA、分公司及其 RA 统称为电子认证服务机构。
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,及 SZCA 设立的代理部分证书业务的业务分支机构。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，及受理点证书发放机构。发证机构为证书申请者发放 SZCA 证书。
CPS 策略发展小组	由 SZCA 任命的负责 CPS 的起草与修订，日常维护管理与咨询的组织。
SZCA 运营安全管理小组	由 SZCA 任命的负责 SZCA 安全策略核准及执行的组织。
SZCA 超级管理员	负责实施 CA 政策、增加新 CA 管理员、验证审计记录、电子认证业务规则的执行情况承诺。
SZCA 系统管理员	负责安装、配置和维护 ，CA 系统的软硬件系统，负责 CA 服务器的启动和中止。
SZCA 录入员	负责录入证书申请者提交的信息。
SZCA 审核员	负责审核证书申请信息。
SZCA 审计员	CA 审计员（Auditor）负责 CA 系统的证书统计，系统审计。
SZCA 证书制作员	负责为证书申请者制作证书。
SZCA 数字证书签发系统	为 SZCA 证书申请者签发、管理数字证书的软件系统。
SZCA 白皮书	SZCA 白皮书是 SZCA 的一个支持 SZCA 数字证书相应政策的详细的

	操作规则和操作步骤。
注册机构协议	一份合同，它详细地概括了 SZCA 指定的注册机构的程序、责任和义务。
注册分支机构协议	一份合同，它详细地概括了 SZCA 指定的注册分支机构的程序、责任和义务。
依赖方	（Relying Party）指基于对数字证书或电子签名的信任而从事有关活动的人。
订户	向 SZCA 申请证书，并持有使用证书，且能为证书使用行为承担责任的实体。
证书申请者	证书申请者（Certificate Applicant）请求 SZCA 颁发证书的个人、企事业单位、及其他组织机构。
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	证书口令指证书中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吊销列表（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。
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	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 信息库

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

2.2 认证信息的发布

SZCA 的 CPS、CP 以及相关的技术支持信息等在 SZCA 网站上发布。SZCA 的 LDAP 服务器发布、更新证书及 CRL 信息。用户证书可通过 SZCA 网站查询或下载证书。已被挂起、吊销的证书的信息可从 CRL 查获；证书的状态（有效、吊销、挂起）可通过 OCSP 服务获得。

SZCA 同时将发布通告与 SZCA 本身证书、服务能力及签发证书相关的重大事件，包括 SZCA 本身证书挂起、吊销或 SZCA 的证书发生影响安全性可靠性的危机事件或其他影响 SZCA 服务能力的重大或紧急事件。

2.3 认证信息的发布时间与频率

2.3.1 CP 及 CPS 的发布时间与频率

《粤港电子签名证书互认证书策略》（以下简称粤港互认 CP）由粤港电子签名证书互认试点工作组发布，本 CPS 依照粤港互认 CP 制定，SZCA 将根据最新的粤港互认 CP 即时同步更新本 CPS。

本 CPS 以及相关业务规则在完成 1.5.4 所述的批准流程后 5 个工作日内发布到 SZCA 的网站，并确保 7*24 小时可访问。

CPS 一经发布，即对订户、依赖方及 SZCA 产生约束力。现行有效正在实施的 CPS，对 CPS 发布前的仍处于有效期的证书的订户，及发布后签发的证书的订户，具有同等效力。

2.3.2 证书及 CRL 的发布时间与频率

证书签发完成后，SZCA 于 24 小时内在本机构的信息库、或其它由订户指定的信息库位置中发布该证书，及定期更新该证书的相关信息。所有被吊销或挂起的证书，其列表 CRL 通过 SZCA 的目录服务器 LDAP 自动发布，更新周期为 24 小时；特殊情况时，也可人工变更并发布最新 CRL。

SZCA 每年至少发布一次本机构证书有关的证书吊销列表，发布具体时间是本机构证书被吊销后的 20 个工作日内，如遇特殊情况，经本机构的合法程序批准，可延迟发布，但最迟不得超过吊销后的 60 个工作日。

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

2.3.3 其他应公开信息的发布时间与频率

对于有关 SZCA 的服务系统的升级改造、迁移或者出现重大异常紧急事故，SZCA 本身的证书的私钥或者订户的证书密钥失密，SZCA 本身的证书被吊销或挂起，SZCA 暂停或者终止业务等重大事件，SZCA 都将在网站上及时发布公告。

至于其他需要通过信息库向公众公布的信息，其公布内容和公布时间与频次等规则由 SZCA 自行决定，但 SZCA 的信息发布将遵循国家法律法规的规定，并保证发布信息行为是即时、高效的。

2.4 信息库访问控制

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

3. 身份标识与鉴定

3.1 命名

3.1.1 名称类型

SZCA 颁发的证书，含有证书颁发机构（即 SZCA）和订户主体的甄别名（Distinguished Name，简称 DN），所以需要对 SZCA 及证书订户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 的证书采用的是 X.509 标准的甄别名命名方法。

表 3.1-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

表 3.2-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）	个人证书	个人姓名（个人合法有效的身份证明文件上使用的姓名）
	机构身份证书	组织机构名称（组织机构有效经营、服

		务资质证明文件上使用的名称）
机构（O）	证书订户所在的机构名称，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，不填	
证件号	订户的法定证件编号（身份证号、统一社会信用代码号），或需按特定规则脱敏处理	

3.1.2 对名称意义化的要求

DN 用于标识证书主体的名称，必须具有一定的意义，可以追溯，并能明确确定证书主体中的个人或组织机构的真实身份。其与证书主体是一一对应的关系，具有唯一性，并且不会出现与其他主体的命名相冲突。

3.1.3 订户的匿名或伪名

证书申请者使用匿名或伪名，将无法通过 SZCA 的身份验证，所以 SZCA 禁止订户使用匿名。SZCA 应使用订户身份证明材料上的真实姓名/名称为订户命名。订户必须提交真实、完整、准确的身份信息材料，否则即使使用伪名通过审核获得证书，后一经发现核实，SZCA 也将吊销该证书，并有权追究其法律责任。

3.1.4 名称的唯一性

原则上，SZCA 为每个订户签发的证书，其中的订户主体的甄别名都是不同的，并且是唯一的。每个主体甄别名唯一地指代唯一的订户，同一订户的多张证书的甄别名可以相同，但是不同订户的主体甄别名必然不同。如果出现两个或以上证书申请者的称谓相同，则 SZCA 会遵循综合标识法，同时结合有效身份证件号码/统一社会信用代码号、住址、邮件地址等信息，在通用名的基础上对每个主体分别作特殊的标记，区分不同的

主体的身份。

3.1.5 商标的标识、鉴别与角色

证书申请人须保证申请中使用的名称，不会侵犯他人商标专用权等知识产权或其他任何合法权利。在必要时，SZCA 可要求证书申请人提供商标注册文件等具有法律效力的名称使用权证明文件。但 SZCA 不核查证书申请人是否对申请使用的名称享有知识产权等权利；亦不会处理因名称引发的相关纠纷。当此类争议出现时，SZCA 有权在认为有必要时驳回、中止处理证书申请或挂起相关证书直到争议解决，且不需对任何证书申请人负法律责任，并根据生效的裁判文书或者和解调解协议等，作出证书名称使用的相关处理。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

证明订户拥有私钥，是通过 pkcs#10 所包含的数字签名方法来完成的。具体来说，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，如果相同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。此外，SZCA 还可以在信赖私钥存储介质和私钥足够安全可靠的条件下，要求其提交私钥原始数据及其存储介质。

3.2.2 订户身份的鉴别

订户在申请证书前应本人或者通过书面授权指定证书的申请代表，提供有效身份证明文件、证书申请文件等申请材料，并签署接受认证服务协议中的有关条款，同意承担相应的责任。

SZCA 受理订户的证书申请后，根据订户提交的身份证明文件等申请材料，对订户的身份真实性进行审核，并按照相关法律法规的要求妥善保存订户申请材料。对订户身份真实性进行鉴别审核，可以通过面对面的当场审查、查询第三方权威可靠数据库以及其他方式来实现。

3.2.2.1 自然人身份的鉴别

SZCA 的个人（即自然人）证书业务，目前仅受理年满 18 周岁、具备完全民事行为能力并定居中国取得中国国籍的个人的证书申请。

自然人订户申请 SZCA 数字证书时，应本人向 SZCA 或其注册机构提交真实、合法有效且完整的身份证明文件及申请表等申请材料。

自然人订户应提交如下材料：

（1）证书申请表与/或服务协议

（2） 有效身份证件[③]复印件或影印件

SZCA 审核检查订户提交材料的完整性、真实性及有效性。并通过可信数据源对订户身份信息、地址信息等进行鉴别。

SZCA 及其授权的注册机构，按照 SZCA 个人身份鉴别规范对申请材料的原件、复印件或其它电子数据的真实性进行审核，并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复印件，与证书申请表，或其它电子数据一并存档保存。

自然人订户身份鉴别的方式，为面对面的审核方式核实订户身份。自然人订户，向 SZCA 申请电子身份认证，须本人持有效身份证件，亲自至 SZCA 或其授权的注册机构的业务受理场所，SZCA 的工作人员通过可靠有效的措施验证身份证件的真实有效性，核对订户与申请材料记载的信息主体（即证书申请者）、订户与身份证件主体等的一致性。

3.2.2.2 组织机构身份的鉴别程序

组织机构在向 SZCA 申请证书时，应指定、授权本机构的工作人员作为证书申请代理人，负责提交包括机构身份证明文件在内的各种申请材料，并在申请表等上签字表示接受证书申请的有关条款，且愿意承担相应的责任。

组织机构申请证书应提交的申请材料有：

（1）证书申请表与/或服务协议；

③ 中华人民共和国居民身份证、户口簿、护照是公民法定身份证件，具有证明公民身份的法律效力。（《关于改进和规范公安派出所出具证明工作的意见》）

（2）机构（法人）身份证明文件的复印件；

（3）申请代理人的个人有效身份证件的复印件（加盖机构公章）；

（4）机构授权申请代理人的授权证明文件。

首先，SZCA 对申请材料进行完整性初步查验，并核对申请代理人与个人身份证件主体信息，订户与机构身份证明文件主体信息、申请表中申请代理人信息与其身份证件主体信息的一致性；

其次，SZCA 对组织机构提供的身份证明材料等，通过可靠的数据源[④]（包括但不限于国家企业信用信息公示系统等）进行真实性、有效性的鉴别。在确定机构的授权申请代理人意愿时，可通过电话、公函、实地走访等方式调查确认。对法定代表人、申请代理人的个人的身份进行鉴别，依照上述自然人鉴别方式进行。

在针对以上申请材料使用上述鉴别方式，SZCA 仍然无法鉴别确认订户身份的，SZCA 有权采取其他认为可靠必要的鉴别手段，或要求订户提交其他额外的证明材料。订户有义务配合 SZCA 提交认证所需的材料，并保证申请材料的真实性有效性及完整性，并积极协助 SZCA 进行身份鉴别。

3.2.2.3 认可的身份证明文件类型

（1）基本身份证明文件的类型

表 3.3-基本身份证件类型

<table>
<tr><th>个人证件类型</th><th colspan="2">机构证件类型</th></tr>
<tr><td rowspan="3">居民身份证</td><td rowspan="4">统一社会信用代码证</td><td>营业执照</td></tr>
<tr><td>事业单位（法人）登记证</td></tr>
<tr><td>政府批文（政府机构）</td></tr>
<tr><td>护照</td><td>社会团体（法人）登记证</td></tr>
</table>

[④] 可靠的数据源： “国家企业信用信息公示系统”（ http://www.gsxt.gov.cn）或“全国组织机构统一社会信用代码数据服务中心”（http://www.nacao.org.cn）

		人民团体（法人）登记证
		外国（地区）企业常驻代表机构登记证

（2）补充性身份证明文件的类型

表 3.4 -补充性身份证件类型

个人证件类型	机构证件类型
临时居民身份证	银行开户许可证
社会保障卡	
银行账户	
户口本	

3.2.3 没有验证的订户信息

SZCA 签发的证书所包含的信息没有未经验证的信息。

3.2.4 授权确认

当组织机构委托第三人作为申请人代理办理具体的证书申请，该代理申请人需向 SZCA 及其授权注册机构，提交证明合法有效授权的书面文件、及其他证明该申请人与组织机构关系的辅助性证明文件。SZCA 先确认组织机构合法存在，并采取电话邮件及实地调查方式，或者通过第三方等其他方式确认该授权的真实有效合法性。

3.2.5 互操性准则

对于申请本 CPS 下的证书订户，SZCA 可委托其注册机构承担对订户身份的鉴别职能，SZCA 将不再进行其他鉴别。

在符合法律法规条件下，对于其他电子认证服务机构，在签订包含对等原则条款等

的合作协议等情况下，SZCA 将接受经其鉴别的订户信息，并为订户颁发证书。一旦 SZCA 与其他电子认证机构合作，相互承认鉴别信息相互签发证书，则 SZCA 将通过官方网站等渠道公布相关证书信息。

3.3 密钥更新请求的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

一般情况下，证书有效使用需满足的条件是：证书在有效期内、证书信息未发生变更及证书安全未失密。SZCA 签发的证书的有效期为一年。SZCA 有权根据具体情况决定证书有效期长短。则在证书内容不变的情况下，如在证书有效期即将届满或到期，订户需要在证书期满后继续使用证书的；或对证书密钥有安全顾虑时，可以申请重新注册、产生新的密钥对，并向 SZCA 申请重新签发证书。

证书密钥需要更新的情形，一般分为两种：

（1）证书补发

证书私钥失密等导致无法继续正常使用，主要是在证书有效期届满之前证书密钥可能失密，包括证书的存储介质丢失或者毁损，私钥发生泄漏被窃取盗用冒用等。

（2）证书换发

主要是证书有效期即将届满或已到期、过期。

对证书密钥更新的申请，SZCA 将对原证书真实性、原证书内容是否变化及申请者的身份等方面进行鉴别，鉴别方式、要求和程序与初始的证书申请身份鉴别方式一致。但除证书或其密钥失密外，订户也可通过 SZCA 签发的初始证书签名并提交证书更新申请，则 SZCA 通过证书公钥对签名进行验证，可适当简化该身份鉴别流程。

在订户密钥更新请求及理由正当，并且能提供有效的据以证明需要更新密钥的文件情况下，SZCA 审核同意后即可为其更新密钥。订户申请密钥更新时，应对所有使用原密钥加密的文件或数据进行解密和保存，否则由此造成的损失，由订户自行承担。

3.3.2 吊销后密钥更新的标识与鉴别

SZCA 不对被吊销的证书的密钥进行更新，证书被吊销后申请密钥更新相当于订户重新申请证书，即证书吊销后对密钥更新的标识与鉴别按照本 CPS 3.2 处理。

3.4 吊销请求的标识与鉴别

对于订户及其代理人提出的证书吊销请求，SZCA 应要求其提供与初始证书申请时相同的身份证明材料，或者使用 SZCA 签发的证书对吊销请求进行有效签名。SZCA 依据以上材料或信息进行身份鉴别。一般来说，SZCA 会当场审核订户信息，核验吊销请求人身份的真实性；当无法进行现场确认时，SZCA 将通过电话邮件或其他第三方可靠证明的方式，对申请者的身份进行鉴别。

对吊销申请的标识与鉴别，只适用于订户提出吊销申请。对于电子认证机构依据充足的事实和理由，以及根据司法机关的证书吊销裁决等作出的证书吊销，只需进行简单的鉴别。但在证书吊销事由调查和核实的过程中，SZCA 有权决定在合理的情况下先行暂时挂起证书，并在身份鉴别结果确定时处理该吊销请求。

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

任何实体，需要使用 SZCA 在《粤港电子签名证书互认证书策略》下签发的证书时，均可向 SZCA 提出证书申请。目前具体包括定居中国的中国公民个人、在中国合法成立且有效存续的企业、事业单位、政府机构、社会团体及其他非法人组织。

4.1.2 注册过程与责任

4.1.2.1 最终订户

最终订户即申请证书的实体，最终订户须明确表示其愿意接受本 CPS 及相关的 CP 中所规定的相关责任与义务（本 CPS 及相关 CP 公布在 SZCA 网站上），并需要按照 3.2.2 的要求提供真实、准确的申请信息；根据《中华人民共和国电子签名法》的规定，申请者未向 SZCA 提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、 SZCA 或者 SZCA 的注册机构造成损失的，订户应承担相应的法律及赔偿责任。

订户有责任保证其拥有的证书私钥安全。SZCA 并不强制性要求证书申请者只能采取 SZCA 规定或提供的安全措施；订户可以选择任何认为可行的保密措施，但由此造成的密保存问题及其损失，订户须自行承担。

订户应按照约定的用途合法使用证书。一旦订户将证书用于违法犯罪目的，或者超越约定范围擅自滥用证书，由此造成的责任，由订户自行承担。

4.1.2.2 认证及注册机构

SZCA 既是一个 CA，同时也承担了部分注册机构的职能，如订户可以直接向 SZCA 申请证书，由 SZCA 审核订户信息并处理订户的请求。同时 SZCA 授权的注册机构及因与 SZCA 合作成为 SZCA 注册机构的第三方机构，受理订户证书申请。注册机构对订户提供的身份信息参照 3.2.2 的要求进行鉴别， SZCA 及 RA 机构对通过鉴别后的订户签发证书。

SZCA 作为电子认证机构，应妥善保管证书订户申请材料及信息。SZCA 的注册机构应在适当时间将证书订户的信息归档在 SZCA，同时应履行本 CPS 中所规定的相关责任与义务，如 SZCA 及其注册机构有义务保证自身认证系统及密钥的安全性。

4.2 证书申请处理

4.2.1 执行识别与鉴定功能

SZCA 处理证书申请至少需要设置三个可信角色：信息收集、信息验证、签发证书。其中信息收集、信息验证可以由同一人或设备[5]完成；但签发证书人员需要与信息收集、信息验证职责分离。

对于证书申请处理，签发证书人员或设备需对申请机构信息做最终审核：

（1）对所有用以验证申请订户证书申请的信息和文件进行复核，查找冲突的信息或需要进一步验证的信息；

（2）如复核人提出的问题确实需要得到进一步验证，SZCA 必须从订户、注册机构、协议签署人、申请审批人或其他合格的独立信息来源取得进一步验证的资料或证据；

（3）SZCA 必须保证已收集的与证书申请相关的信息和资料，足以确保签发的证书不包含 SZCA 已知或应发现的错误信息，否则 SZCA 将会拒绝证书的申请并通知订户；

如果 SZCA 委托其他机构担任 RA 角色，对于 RA 验证后的申请，SZCA 负责最终验证。

4.2.2 证书申请的批准与拒绝

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

[5] 设备指身份证明文件及现场申请人影像等专有采集、识别、判断的设备或计算机程序。

4.2.3 处理证书申请的时间

在申请者所提交的证书申请材料齐全完整并符合要求的情况下，SZCA 或授权的发证机构将 24 小时内申请信息进行审核，因特殊原因需要延长的，将及时通知申请者并说明理由。

4.3 证书签发

4.3.1 证书签发中注册机构和电子认证服务机构的行为

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

4.3.2 电子认证服务机构及注册机构对订户的通告

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

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 授权的发证机构将向申请者提供证书、或证书的获取渠道。证书申请者通过上述方式获得证书后，应检查、测试使用证书是否存在信息错误等问题，若发现证书内容及密钥安全等问题，应在 2 个工作日内 SZCA 发出通知，要求更换新证书。订户在获得证书起的 2 个工作日内未提出异议或提出的异议不成立时起即被视为已接受证书。证书申请者接受数字证书后，应妥善保存其证书对应的私有密钥。

4.4.2 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证书信息库（目录服务器 LDAP 及 OCSP）中，供订户和依赖方查询和下载。

4.4.3 电子认证服务机构对其他实体的通告

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

4.5 密钥对与证书的使用

4.5.1 订户私钥与证书的使用

订户的私钥和证书应用于法律、CPS 规定的、或服务协议约定的用途（在本 CPS1.4.1 节定义），不得将证书用于实施违法犯罪活动；订户在使用证书时必须遵守本 CPS 的要求，妥善保存其私钥，保持本人对私钥的控制，采取合理的措施防止私钥遗失、泄露、被篡改，避免他人未经本人授权而使用本人证书情形的发生，否则其应用是不受保障的。

证书持有者只有在接受了相关证书后才能使用对应的私钥，且只能在指定的应用范围内使用私钥和证书；证书持有者在证书到期不续费或被吊销后，须停止使用该证书对应的私钥。订户在发生无法确定证书及其私钥是否安全的事件或意外时，应立即通知 SZCA 吊销该证书。

订户使用证书私钥签名，即保证是以订户本人名义进行的签名，且在进行签名时证书未过期、未被挂起或吊销。

4.5.2 依赖方公钥与证书的使用

依赖方信赖 SZCA 在《粤港电子签名证书互认证书策略》下签发的证书所证明的信任关系时，需要：

（1）获得数字签名对应的证书和信任链；

（2）查询 CRL 或 OCSP，确认数字签名对应的证书有效、状态正常；

（3）确认证书是依赖方信任的证书；

（4）证书的用途适用于对应的签名；

（5）使用证书上的公钥验证签名。

以上任一条件不满足或步骤操作失败，依赖方应该拒绝接受签名信息。

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 证书密钥更新

证书密钥更新，是指在证书订户信息不变的情况下，为订户生成新密钥并为新公钥签发新证书。

4.6.1 证书密钥更新的情形

（1）当订户证书即将到期或已经到期时；

（2）当订户证书密钥遭到损坏时；

（3）当订户证实或怀疑其证书密钥不安全时；

（4）其它可能导致密钥更新的情形。

4.6.2 请求证书密钥更新的实体

同本 CPS 4.1.1。

4.6.3 证书密钥更新请求的处理

订户在证书有效期满前 30 天申请证书更新的，或证书密钥已确认失密或可能失密的，应向 SZCA 申请证书密钥更新。

证书密钥更新处理程序如下：同本 CPS 3.3。

新证书签发后，旧的证书被吊销。

4.6.4 颁发新证书时对订户的通告

同本 CPS 4.3.2

4.6.5 构成接受密钥更新证书的行为

同本 CPS 4.4.1。

4.6.6 电子认证服务机构对密钥更新证书的发布

同本 CPS 4.4.2

4.6.7 电子认证服务机构对其他实体的通告

同本 CPS 4.4.3

4.7 证书变更

证书变更是指在证书未到期之前，证书除公钥及有效期之外的其他订户信息发生变化而重新办理证书。SZCA 的认证业务不直接支持证书变更。订户证书内容变化且订户申请变更证书的，视为申请一张新证书，需要先将原有证书吊销，才能申请新证书，且证书的申请及处理流程与申请新证书一致。

目前 SZCA 不接受本 CPS 自然人订户证书变更。

4.7.1 证书变更的情形

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

4.7.2 请求证书变更的实体

同本 CPS 4.1.

4.7.3 证书变更请求的处理

同本 CPS 4.2。

原证书的吊销程序，依照证书强制吊销程序操作。

证书变更后，证书的有效期无变化，与原证书的有效期相同。

4.7.4 颁发新证书时对订户的通告

同本 CPS 4.3。

4.7.5 构成接受变更证书的行为

同本 CPS 4.6.5

4.7.6 电子认证服务机构对变更证书的发布

同本 CPS 4.6.6

4.7.8 电子认证服务机构对其他实体的通告

同本 CPS 4.4.3

4.8 证书吊销与挂起

证书吊销是永久性证书失效与禁用，不可以进行证书恢复。而证书挂起则是证书暂停使用的一种临时性状态，经 SZCA 调查后确认恢复正常使用状态或吊销证书，是一种应对可能出现证书使用安全风险或证书效力异常时的过渡性临时应急止损措施。

4.8.1 证书吊销的情形

4.8.1.1 订户证书吊销的情形

如有下列情况中的任何一种情况发生，则订户的证书将被吊销：

（1）订户书面申请吊销数字证书；

（2）因申请证书密钥更新导致的；

（3）订户未支付证书费用；

（4）订户通知 CA 且有证据证明初始的证书申请未获有效授权；

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

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

（7）当 CA 有证据表明订户未履行本 CPS 或订户协议中约定的义务；或者订户证书不符合本 CPS 的相关要求；

（8）SZCA 发现且有合理证据证明订户证书中的重要信息内容已经变更；

（9）CA 签发的证书未能满足证书策略或证书标准中的要求和条件；

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

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

当 SZCA 从事电子认证业务的资格证书被吊销后，SZCA 除继续维持 CRL/OCSP 信息库的情况外，将吊销或终结所有已签发的证书；

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

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

（14）证书的重要参数被国际国内主流标准认为有重大风险时；

（15）法律、行政法规规定的其他情形。

4.8.1.2 SZCA 本身证书吊销的情形

CA 本身的密钥（包括本身即子 CA 的密钥）的安全性被破坏或怀疑有遭受破坏损害

的可能性时，向工信部等监管部门提出吊销申请。

4.8.2 请求证书吊销的实体

已申请 SZCA 证书的订户可请求证书吊销。

同时，SZCA 也可在 4.8.1 所述的情形下强制吊销订户的证书。

4.8.3 申请证书吊销的程序

吊销分为主动吊销和被动吊销。

主动吊销是指由订户提出吊销申请，由 SZCA 审核通过后吊销证书的情形；

被动吊销，又称强制吊销，指 SZCA 在发现 4.8.1 除第一项外的情形，且订户未提出吊销请求的情况下，因订户的违法使用证书、密钥失密或证书信息发生重大变化等原因，直接决定吊销证书。或者 SZCA 或其授权发证机关等根据司法机关的裁决，进行调查核实后吊销证书。

但对于此种非经订户申请吊销的强制吊销，SZCA 或其发证机构将对相关的裁判文书及其他有效法律文件进行严格核验，并在机构内部经过至少两级的逐层审批，并由高级管理人员完成最终审批。

4.8.3.1 主动吊销

订户申请吊销证书前应指定并书面授权证书吊销申请代表，提供有效身份证明文件及证书吊销申请文件，并接受证书吊销申请的有关条款，同意承担相应的责任。

SZCA 7X24 接受订户证书吊销申请，并处理订户证书吊销请求。

订户可通过 SZCA 7X24 热线、SZCA 在线服务等方式提出申请。SZCA 收到订户的吊销申请材料后，将查询订户需吊销的证书是否为 SZCA 所发放，证书是否在有效期内，吊销理由是否属实，并同时对吊销申请人的身份进行鉴别（仅适用于主动申请吊销），若均通过则对证书进行吊销。

4.8.3.2 被动吊销

无论是 SZCA 主动发现，还是经司法机关仲裁机构、依赖方、软件供应商向 SZCA 反

映且调查属实时，当出现证书须吊销的情形时，SZCA 将以适当形式通知订户，告知拟吊销的证书内容、吊销原因、吊销操作时限等事项，在确认订户收到吊销通知且无异议后予以吊销。

4.8.4 申请证书吊销的宽限期

在主动吊销的情形下，订户一旦发现需要吊销证书，应及时向 SZCA 提出吊销请求。在被动吊销的情形下，订户在收到吊销通知后的三个工作日内可向 SZCA 提出异议，但需同时说明理由或提供证据，SZCA 将会对异议进行审查，若确认其理由正当则不予以吊销；若订户在三个工作日内未回复、无异议或异议不成立的，则 SZCA 将予以吊销。

因订户未及时提出吊销请求而产生的任何损失和责任，SZCA 并不承担。

4.8.5 电子认证服务机构处理吊销请求的时限

在主动吊销的情形下，SZCA 收到吊销请求并审核完成后，二十四小时内吊销证书。

在被动吊销的情形下，订户在收到吊销通知后的三个工作日内可向 SZCA 提出异议，SZCA 将会对异议进行评估，若确认其理由正当则不予以吊销；若订户在三个工作日内未回复、无异议或异议不成立，则 SZCA 将于二十四小时内予以吊销。

4.8.6 依赖方检查证书吊销的要求

依赖方在信任此证书前应检查证书的有效性，确认证书未被吊销。依赖方在信任证书前根据 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。如果 CRL 公布证书已经吊销，而依赖方没有查 CRL，由此造成的损失由依赖方承担。

4.8.7 CRL 发布频率

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

4.8.8 CRL 发布最大滞后时间

CRL 发布的最大滞后时间为二十四小时。

4.8.9 在线证书状态查询的可用性

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

SZCA 的 OCSP 系统查询未设置任何读取权限。

SZCA 提供 OCSP 查询服务，服务 7X24 小时可用。信赖方是否进行在线状态查询完全取决于信赖方的安全要求。对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，信赖方在信赖一个证书前可通过证书状态在线查询系统检查该证书的状态。

SZCA 的 OCSP 响应符合 RFC2560 标准。客户通过 http 协议访问 SZCA 的 OCSP 服务， SZCA 会对查询请求进行检查，检查的内容包括：

(1) 验证是否强制请求签名；

(2) 用 CA 证书验证签名是否通过；

(3) 验证证书是否生效或者已经过期；

(4) 验证证书颁发者是否在信任证书列表内。

表 4.1-OCSP 响应包含如下表所述基本域和内容

域	值或者值得限制
状态	响应状态，包括成功、请求格式错误、内部错误、稍候重试、请求没有签名和请求签名证书无授权，当状态为成功时必须包括以下各项。
版本	V1
签名算法	签发 OCSP 的算法。Sha1RSA、sha256RSA、sm3SM2 算法签名。
颁发者	签发 OCSP 的实体。签发者公钥的数据摘要值和证书甄别

	名。
产生时间	OCSP 响应的产生时间。
证书状态列表	包括请求中所查询的证书状态列表。每个证书状态包括证书标识、证书状态以及证书废止信息。
证书标识	包括数据摘要算法、证书甄别名数据摘要值、证书公钥数据摘要值和证书序列号。
证书状态	证书的最新状态，包括有效、吊销和未知。
证书废止信息	当返回证书状态为废止时包含废止时间和废止原因。

OCSP 的扩展信息与 RFC2560 一致。SZCA 的 OCSP 信息的更新频率不超过 24 小时， OCSP 服务响应最大时间不超过 10 秒， OCSP 服务响应信息最大有效期不超过 7 天。

4.8.10 吊销信息的其他发布形式

证书吊销信息可以通过 CRL 或者 OCSP 服务获得。订户可通过证书扩展域中的 CRL 地址获得 CRL 信息。

4.8.11 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发起证书吊销。

4.8.12 证书挂起的情形

如有下列情况中的任何一种情况发生，则 SZCA 经对订户的证书将进行挂起处理：

（1）订户书面申请挂起数字证书；

（2）当 CA 有证据表明订户将证书使用于法律、行政法规定义为非法事项上，或者 CA 发现订户证书未恰当使用；

（3）当 CA 有证据表明订户未履行本 CPS 或订户协议中约定的义务；或者订户证

书不符合本 CPS 的相关要求；

（4）SZCA 发现或有合理证据证明订户证书中的重要信息内容已经变更，且订户未申请证书变更；

（5）CA 认定证书中所显示的信息为不真实准确或具有误导性；或者订户申请证书时，提供的资料不真实；

（6）法律、行政法规规定的其他情形。

4.8.13 请求证书挂起的实体

参照本 CPS 4.1.1

4.8.14 请求证书挂起的程序

挂起分为主动挂起和被动挂起。

主动挂起是指由订户提出挂起申请，由 SZCA 审核通过后吊销证书的情形；

被动挂起是指当 SZCA 确认订户违反证书应用规定、约定或证书中订户有关信息发生变化等情况发生时，先行采取挂起证书的手段，等待订户或订户受托人对证书吊销的反馈，及 SZCA 对各种证书挂起、吊销事由进行调查后的最终处理。

4.8.14.1 主动挂起

订户申请挂起证书前应指定并书面授权证书挂起申请代表，提供有效身份证明文件及证书挂起申请文件，并接受证书挂起申请的有关条款，同意承担相应的责任。

SZCA 7X24 接受订户证书挂起申请，并处理订户证书挂起请求。

订户可通过 SZCA 7X24 热线、SZCA 在线服务等方式提出申请。SZCA 收到订户的挂起申请材料后，将查询订户需吊销的证书是否为 SZCA 所发放，证书是否在有效期内，则对证书进行挂起。

4.8.14.2 被动挂起

当出现被动挂起的情形时，SZCA 将以适当形式通知订户，告知拟挂起的证书内容、挂起原因、挂起操作时限等事项。

4.8.15 请求挂起的期限限制

SZCA 根据订户的申请，或对吊销事由的调查结果，在证书到期前对挂起的证书进行恢复或吊销的操作。

4.8.16 证书挂起的恢复程序

订户恢复挂起证书前应指定并书面授权证书恢复挂起申请代表，提供有效身份证明文件及恢复证书挂起申请文件，并接受证书挂起申请的有关条款，同意承担相应的责任。

SZCA 7X24 接受订户证书恢复挂起申请，并处理订户证书挂起请求。

订户可通过 SZCA 7X24 热线、SZCA 在线服务等方式提出申请。SZCA 收到订户的恢复挂起申请材料后，将查询订户需挂起的证书是否为 SZCA 所发放，证书是否在有效期内，恢复挂起理由是否属实，若均通过则对证书进行恢复。

4.9 证书状态服务

4.9.1 操作特征

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

4.9.2 服务可用性

SZCA 提供 7X24 小时的证书状态查询服务，并尽量降低减少服务中断时间。对于因事故演练、系统升级改造等内部原因需要安排暂时中断该证书在线状态查询服务的，也应确保中断时间每星期不超过两个小时；而对于非 SZCA 可控的意外事故或不可抗力造成的服务中断，SZCA 也应尽力修复恢复该服务。一旦出现 SZCA 证书状态服务中断，则 SZCA 应尽快将该中断事项通知有关各方。

4.10 订购结束

订购结束的情形有以下两种：

（1）证书到期时且不续费申请使用其他证书服务；

当证书到期时，证书使用者不续费不申请更新证书或证书密钥，不再使用 SZCA 证书。

（2）证书有效期内吊销证书。

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

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

② 或者司法机关裁决吊销证书，并向 SZCA 提出执行请求；

③ SZCA 强制吊销该证书。

4.11 密钥生成、备份与恢复

4.11.1 签名密钥的生成、备份与恢复的策略与行为

硬介质证书，订户签名密钥对由订户的密码设备生成，由订户自行保管。SZCA 可经订户委托代为进行签名密钥对生成的操作，但 SZCA 承担相应的保密责任，SZCA 不对签名密钥进行任何备份或保存；SZCA 不接受订户签名密钥的托管，不提供签名密钥恢复服务。

订户应妥善保管签名密钥，对其进行备份，并保证使用的安全性，由于签名私钥遗失所造成的损失由订户自己承担，SZCA 概不负责。

SZCA 不负责恢复订户签名密钥。

4.11.2 证书托管服务

SZCA 本身的密钥不能被托管。

4.11.3 加密密钥的生成、备份与恢复和策略与行为

证书订户的加密密钥由国家密钥管理中心生成，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、司法调查取证的需要；

只有在国家相关法律的明确规定的情况下才能进行此类密钥恢复。且申请者要提供有关证明文件、材料及说明合理的理由。

（3）密钥管理中心认为有必要。

5.认证机构设施、管理和操作控制

5.1 物理控制

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

SZCA 实施功能分区及其访问控制制度，操作人员要进入、操作相应的管理区域及其他关键核心区域；且对该区域的设备与系统日常运行及人员操作过程进行监控。SZCA 的根密钥置于最高安全强度保护环境与状态，防止任何非法破坏或者未经授权的操作。

5.1.1 场地位置与建筑

SZCA 认证系统的主机房位于深圳市南山区高新中二路深圳软件园 8 栋三楼，机房按照功能分为业务受理区、辅助设备区、服务区、RA 管理区、CA 管理区、CA 核心区、KM 管理区、KM 核心区。各功能区域对应的安全区域，实施不同的安全等级控制制度，SZCA 采用门禁控制、视频监控等多种有效的物理安全控制措施。机房具备抗震、防火、防水、恒湿温控、防电磁干扰与辐射、备用电力等功能，保障服务的连续性、可靠性。

5.1.2 物理访问

访问进入机房等敏感区域，必须通过 IC 卡门禁系统和指纹识别系统等的身份检验，并且工作人员对机房中的设备进行操作，还需通过权限验证，且要严格按照操作规程进行，且操作过程经 24 小时监控设备监控。

而非法闯入或进出入超时等各种访问异常情况都会出发报警系统。门禁系统记录所有访问时间等访问信息。SZCA 将定期对该门禁进出记录进行整理归档。且该门禁进出记录将保存至少 3 个月。

机房配备有监控系统，对基础设施设备、机房环境状况、安防系统状况及访问操作情况进行 7*24 小时的实时监测。对高级设备要进行 24 小时自动监控或人工监视。且监测记录应至少保存 3 个月，能满足故障诊断、事后审计的需要。

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，保障紧急情况也能持续不间断供电。

系统机房使用中央空调,进行温度和湿度的调控；且装置有换气设备，对机房进行换气，保证机房内的空气质量、温湿度、新风供应以及空气清洁度等均达到国家规定的标准。

5.1.4 水患防治

SZCA 的机房位于大楼三楼，认证服务系统所处的环境为密闭式，并且安装水浸自动报警系统等，对水灾进行监测、预警，降低预防水害对系统的影响。

5.1.5 火灾预防

SZCA 机房内安装有火灾自动报警系统及气体自动灭火系统。且火灾报警系统与灭火系统联动触发运作。火灾自动报警系统设置有两种火灾探测器以检测温度和烟雾。气体自动灭火系统支持自动、手动及机械应急操作等三种启动方式。

火灾报警系统的火灾探测器检测到机房内温度及烟雾异常，火灾报警器发出双报警信号，火灾报警控制器发出动作信号启动灭火系统；当工作人员处于火灾系统防护区域的，可以把灭火系统切换到手动触发模式；在自动启动、手动启动失灵时，可以启动机械应急操作方式。

5.1.6 介质存储

SZCA 对存储有系统软件、归档数据、备份数据及其他重要敏感数据的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。并采取介质使用登记注册、介质防复制及信息加密等措施实现对介质的安全保护，防止介质被认为破坏、或未经授权的使用、访问、被披露。

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，设备内敏感性和机密性信息都将被做安全且不可恢复的彻底的清除。存储或传输介质，应做特殊的销毁或不可读的处理。密码设备在作废处置前根据加密机管理办法及生产制造商的指导将其物理销毁或初始化。

所有处理行为遵守我国有关的法律法规信息，并将记录在案。

5.1.8 异地备份

SZCA 对关键系统、重要软件和重要业务数据（包括审计数据在内的任何敏感信息）进行异地备份，遇到灾难情况发生时启用备份数据，保证系统正常提供服务。

5.1.9 时间戳服务器证书物理控制

SZCA 独立控制并运营时间戳服务器，其密钥保存在加密机中， SZCA 确保时间戳服务使用的私钥被保存在符合 FIPS-140-2 级别或者更高级别的加密机中，SZCA 时间戳服务提供的时间源为中国科学院国家授时中心（位于陕西天文台），时间对应为国际标准 UTC 原子钟。

5. 2 程序控制

5.2.1 可信角色

可信角色，是指 SZCA 及其授权注册机构等组织中，与密钥和证书生命周期管理操作有关的角色，可能会对以下几个方面产生重要影响的人员，包含但不限于：

(1) 证书申请中信息验证与确认；

(2) 对证书申请、吊销进行批准、拒绝或其他操作；

(3) 证书签发和吊销；

(4) 对严格控制访问的信息库进行访问；

(5) 控制、操作 SZCA 密钥及密码设备；

(6) 处理订户信息或请求等

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：

(1) SZCA 运营安全管理小组

(2) SZCA 超级管理员

(3) SZCA 系统管理员

(4) 系统审计员

(5) 密钥管理员

(6) 安全管理员

(7) 网络管理员

(8) 监控管理员

(9) 门禁管理员

(10) 录入员

(11) 审核员

(12) 制证员

5.2.2 每个角色需要的人数

表 5.1-可信角色最低人数配备

序号	可信角色	人数
1	运营安全管理小组	3-5
2	超级管理员	2
3	系统管理员	2

4	系统审计员	1
5	安全管理员	1
6	网络管理员	1
7	监控管理员	1
8	门禁管理员	1
9	密钥管理员	3 人以上
10	录入员	若干
11	审核员	2 人以上
12	制证员	2 人以上

SZCA 执行关键操作和岗位职责分割制度，对于敏感操作，如访问、操作和管理密码设备及其密钥，需要至少 3 名可信角色共同完成；操作证书签发系统，需要至少 2 名以上可信角色共同完成；审核及签发证书，也分别至少需要 2 名可信角色共同完成。

5.2.3 每个角色的识别与鉴定

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

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）发放的安全令牌仅限本人使用；

（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等。

对 SZCA 系统设备的逻辑和物理访问等敏感操作应至少由 2 个以上的可信人员参与；对于硬件密钥设备的访问应由至少 3 个以上可信人员共同完成。至少 2 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。掌握系统设备物理访问权限的人不能再享有对系统设备的密钥进行分割的全息。

5.3 人员控制

5.3.1 资质条件

要担任 SZCA 的相关可信角色，须提供相关的教育背景、资历证明等背景信息证明，并具有足以胜任其工作的专业知识、技能及相关经验，且没有相关的不良记录。

5.3.2 背景调查程序

在征得被调查人同意后，SZCA 将对拟录用人员和已录用的正式员工进行严格的可信背景调查，未通过可信背景调查的，一律不得录用；已经录用的一旦发现考核不合格，也将辞退。可信人员背景调查及信誉调查定期进行，原则上 3 年一次，SZCA 根据实际情况可增加调查次数。

SZCA 的员工背景调查，根据应聘者提交的有关个人教育状况、工作经历、资信证明、专业资质能力、政治状况、遵法守纪情况、家庭背景及其他社会关系等各方面信息的证明材料，由 SZCA 人事部门通过包括但不限于调阅档案、电话、邮寄或实地走访应聘者过往就读学校及工作单位等各种符合法律规定的方式，核实材料的真实性。在结合至少 3 个月的试用期的笔试、工作表现及生活方式态度等的考核，判断该人员是否具备胜任该可信角色的能力和条件。一旦通过背景调查，SZCA 将与该人员签订保密协议。

根据被调查人拟担任或已担任的角色的重要性程度，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。应聘人员应提供以下资料：个人履历、最高学历证明、资格证及身份证等相关有效证明。

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

（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。

（4）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。

（5）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。

（6）SZCA 与所有的员工签订保密协议，劳动合同关系存续期间或员工离职日起 2 年内仍然不得从事与 SZCA 相类似的工作。

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 对员工提供包括但不限于以下内容的综合性培训：

（1）公司文化及各类管理制度，如 SZCA 运营体系；

（2）计算机、互联网安全管理制度、安全事故处置措施及程序；

（3）专业知识培训，如 PKI 技术基础、CP 及 CPS 培训；

（4）岗位职责及岗位技能培训；

（5）电子认证相关法律等。

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，不断提高员工专业知识水平与职业技能。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，轮换周期与顺序视具体情况而定。

5.3.6 未授权行为的处罚

SZCA 一旦发现员工涉嫌进行未授权或越权操作，会立即采取如将作废、冻结门禁卡、密钥登录口令、安全证书和 IC 卡等措施，终止该人员访问、操作系统及设备的权限。在行为性质调查属实定性后根据情节严重程度，按照公司规章制度进行处罚；构成犯罪的，公司将采取包括提交司法机关等处理措施。

5.3.7 独立合约人的要求

SZCA 根据自身的业务发展或技术需要，可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，该服务人员须提供相应的身份证明、学历证书、资质证书等有效证明，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，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、联系人等信息；

(3) 证书生命周期的各项操作，包括证书申请、证书及密钥的产生、发出、分派、储存、备份、挂起、吊销、证书密钥更新、存档、销毁及其他有关等事件；

(4) 系统、网络安全事件，包括密钥资料泄露、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) 计算机设施的开发、运营维护记录；

(6) 人员访问控制记录，包括对密钥生成设备及资料的访问；

(7) 密码设备的采购、安装、使用、解除运作及弃用；

(8) 系统巡检记录。

这些记录，无论是手写、或电子文档形式，都应包含事件日期、事件的内容、事件的发生时间段、事件相关的实体、事件的类型及序列号等标识等。

SZCA 记录其它与 CA 系统本身不相关的事件，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 每月定期对各种事件记录进行审查，发现任何安全及管理方面的问题、异常事件，将及时采取补救及处理措施，且对调查审计行为进行记录备案。

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 2 个月，离线存档至少 7 年；并定期检查审计日志。

5.4.4 审计日志的保护

SZCA 采取物理和逻辑安全控制方法，确保审计日志及记录处于严格的保护状态，并对审计日志进行异地备份；禁止未经授权的任何访问、浏览读取并禁止任何修改和删除等操作。

5.4.5 审计日志的备份

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，通过各种备份工具对审计日志和记录按在线和离线进行各种不同形式的备份，且至少每两个月一次定期对审计日志进行备份。

SZCA 也将对审计日志进行归档，归档后原始记录至少保存 5 年。

5.4.6 审计数据、记录的收集

应用程序、网络和操作系统等都会自动生成审计数据和记录信息。

5.4.7 对导致事件实体的通告

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

5.4.8 脆弱性评估

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

5.5 记录归档

5.5.1 归档记录的类型

SZCA 将对总要的事件记录进行归档保存，重要记录包括但不限于：

证书系统建设和升级文档；

(1) SZCA 发行的证书、CRL；

(2) 审计日志；

(3) 证书申请及身份验证、审批信息、订户协议；

(4) 证书策略及电子认证业务规则文档；

(5) 员工资料，包括但不限于背景调查、录用及培训等；

(6) 各种内外部评估文档；

(7) 其他 SZCA 认为重要的文档。

进行归档时 SZCA 将验证所有归档记录的一致性，也将保存该记录的准确时间信息，包含记录产生的日期和时间。

5.5.2 归档记录的保存期限

SZCA 的归档文件的保存期限为：证书或密钥失效后 10 年。

5.5.3 归档文件的保护

SZCA 将各种电子、磁带、纸质形式的归档文件，保存在安全可靠的系统或场所内，且建立和执行安全的物理和逻辑保护措施和严格的管理程序，确保已归档的文件不会被损坏，防止非授权的访问、修改、删除或其它的非法操作行为。

在归档记录的保存期间内，SZCA 保证所有归档记录可以被有效访问，并且采取存储介质和应用软件等方面的措施进行适当的逻辑和物理访问控制，保证只有获授权人员才能访问所有归档记录。并采取适当的方法或技术手段将对所有访问记录的一致性进行

验证。

5.5.4 归档文件的备份

所有存档文件的数据，包括系统生成的电子归档文件，除了保存在 SZCA 的数据库中，还将备份文件进行异地存放。备份归档文件的数据库实行严格的访问控制制度，只有授权人员获非可信任人员在受监督下才能读取档案，禁止对档案及其备份进行删除、修改等操作。

5.5.5 记录时间戳的要求

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 CPS 6.3.2 中规定的最大有效期时，SZCA 将启动密钥更新流程。SZCA 在根证书到期前的 60 天内，停止使用旧证书签发新的下级 CA 证书。但仍可使用旧根证书签发 CRL。SZCA 将启用新的 CA 密钥对签发证书，保证证书链和密钥对顺利过渡，尽量降低因密钥更替对订户和依赖方造成的影响。

5.7 损害与灾难恢复

当 SZCA 遭到攻击，发生通信网络资源崩溃、毁坏、故障，及计算机设备系统不能正常提供服务，软件被破坏，数据库被篡改等情形或因不可抗力造成 SZCA 机房服务暂停或瘫痪时，SZCA 将依照《SZCA 灾难恢复计划》规定的事故处理、紧急应变、灾难恢复和业务持续运作的程序和应对措施实施恢复，尽量至少保证证书状态服务不间断可用，

并可能减少中断时间，通知时说明告知证书挂起及吊销服务中断的时间，及时对系统及设备进行维护及更新。

SZCA 应定期对灾难恢复和业务持续运作的应对措施进行演练，并对演练程序和结果进行记录，应对措施中包含的所有有关主要人员都应参与演练。

5.7.1 事故或损害处理程序

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

5.7.2 计算机资源、软件或数据的损坏

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

5.7.3 实体私钥损害处理程序

SZCA 的根私钥及 SZCA 下级子 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 将按照《SZCA 根私钥泄露紧急处理流程》的相关程序进行处理，及时上报行业主管部门，说明发生时间、原因及采取的应急处理措施，并通知订户和依赖方，吊销所有证书，并停止证书签发行为。

5.7.4 灾害后的业务连续性能力

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

5.8 电子认证服务机构或注册机构的终止

5.8.1 CA 机构业务终止

SZCA 终止业务的原因，可以分为私钥原因和非私钥原因，前者因为 SZCA 本身的密钥失密，而导致 SZCA 无法正常提供证书服务；后者，可能是由于 SZCA 由于电子认证业务密钥使用证书、电子认证服务许可证等证书到期无法换证等资质方面的原因，或其他 SZCA 本身的业务发展需要。当 SZCA 准拟终止或者暂停业务时，应按照法律规范要求，在暂停或终止业务前 90 日尽快作出努力与其他认证机构达成业务承接安排，转交认证相关的材料信息，并将上述事宜通知有关订户、依赖方及注册机构各方，进行相关的赔偿事宜；并在终止或暂停服务前 60 日向工信部报告；不能对业务承接事项作出妥善安排的，应尽快报告工信部按照其要求开展业务承接事宜。

在拟暂停或终止业务期间，SZCA 也将对归档文件及其存储介质、软硬件及其系统进行相应的处理，保证信息的安全及仍在有效期的证书正常使用。

5.8.2 RA 机构业务终止

SZCA 授权的注册机构，暂停或终止业务时，其业务承接安排及通知相关参与方的程序与 SZCA 的业务承接安排程序与通告程序类似，但不同的是业务承接安排是由 SZCA 完成或者 RA 按照 SZCA 的指令进行，RA 无业务承接的自主权；RA 应通告证书订户、依赖方及 SZCA，而向工信部的通报则是由 SZCA 完成。

一般来说，当 SZCA 终止或暂停业务时，其授权的 RA 也将随之终止或暂停业务。另外，SZCA 还有权决定终止或暂停任一或多个 RA 的运营服务，此时其业务承接安排将按照 SZCA 的要求执行，并且相关证书数据及归档文件信息等须于 SZCA 规定的时间内转交给 SZCA 或其指定的其他 RA。

6.认证系统技术安全控制

6.1 密钥对的生成与安装

6.1.1 密钥对的生成

密钥对包括加密密钥对和签名密钥对。

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。

选择硬介质证书订户的签名密钥对由订户的终端自行生成，订户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加密设备、介质生成签名密钥对。签名密钥存储在介质中不可导出，保证 SZCA 无法复制签名密钥对。选择软介质证书订户的签名密钥，由 SZCA 后台密码设备生成，离散加密存储，并保障订户密钥存储及传输的安全。订户有责任保证密钥生成的可靠性，并妥善保管私钥。SZCA 经订户委托可以代为生成密钥对，但承诺不保存密钥对的任何副本。除订户以外的其他机构不应当保存任何订户私钥的副本。

6.1.2 私钥发送给订户

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。

硬介质证书订户的签名密钥对，由订户自己的密码设备生成，无需传送并由订户自行保管。

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

SZCA 采用的介质技术是用于存储证书及私钥的介质技术符合《粤港两地电子签名证书互认技术标准列表和采用措施》的规定。且也对存储密钥的介质的预备、启动、使用、分派及终止使用指定有程序和安全控制措施。

订户的私钥和私钥激活数据，SZCA 将采取不同的方式分发给订户。

SZCA 将记录每次私钥的分发记录。

6.1.3 公钥发送给证书签发机构

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，保证传输中数据的安全。

6.1.4 电子认证服务机构公钥传送给依赖方

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

6.1.5 密钥的长度

SZCA 所使用的密钥对长度支持 RSA2048 SHA256 位，以及国家密码管理局要求的密钥长度。

6.1.6 公钥参数的生成与质量检查

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、介质、模块或加密设备产生。

6.1.7 密钥使用目的

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

订户的签名密钥可以用于提供信用保证和信息安全服务，例如身份认证、不可抵赖性和信息的完整性等；加密密钥对可以用于信息加密和解密，保证网络信息传输安全，防止信息被非法拦截、窃取或篡改。签名密钥和加密密钥配合使用，可实现身份认证、

授权管理和责任认定等安全机制。

6.2 私钥保护与密码模块工程控制

6.2.1 密码模块标准与控制

SZCA 使用国家密码管理局许可的密码产品、设备，密码模块的标准符合国家法律规范规定的要求和《粤港两地电子签名证书互认技术列表和采用措施》的规定。其安全性达到以下要求：

（1）接口安全：不执行规定命令以外的任何命令和操作；

（2） 协议安全：所有命令的任意组合，不能得到私钥的明文；

（3）密钥安全：密钥的生成和使用必须在硬件密码设备中完成；

（4）物理安全：密码设备具有物理防护措施，任何情况下的拆卸均立即销毁在设备内保存的密钥。

SZCA 就产生密钥的工具的采购、接收、安装、验收测试、调试、使用、维修、保养及弃用等制定有效的程序及控制措施，包括但不限于：

（1）保密码模块的完整性；

（2）产生密钥的工具由获授权的人员在适当的督导下操作，防止工具遭擅自改动；设立控制机制，以确保密码模块不会在不能侦测的情况下被擅自改动；

（3）使用密码模块产生的密钥的强度，是符合电子认证服务机构及订户使用密钥的目的所需的适合强度，也符合《粤港两地电子签名证书互认技术标准列表和采用措施》内关于电子签名有关密码算法的规定；

（4）在不同密码模块之间传输密钥时，不会发生私钥丢失、失窃、泄露、被篡改或者未经授权的被使用；

（5）电子认证服务机构的私钥需要在密码模块中以加密方式保存。

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。SZCA 将使用和操作私钥所需的激活数据分割成若干部分，由并经管理层授权的密钥管理人员或操作人员分别持有保管，且必须至少 2 名以上前述人员共同进行，才能完成对加密机中的密钥的管理（生成、激活、备份、恢复及销毁）操作。

6.2.3 私钥托管

对于 CA 密钥 SZCA 无托管业务；

6.2.4 私钥备份

CA 的私钥保存在防高温、防潮湿及防磁场影响的环境中，对私钥的备份操作必须 3 人以上（包括 3 人）才可完成。

SZCA 每天对 CA 的私钥进行备份。

RA 的私钥由 RA 产生，由 RA 自行备份。

订户的签名私钥有订户产生，建议订户自行备份，并对备份的私钥采用口令或其他访问控制机制保护，防止非授权的修改和泄漏。SZCA 不对订户的加密私钥进行备份。

6.2.5 私钥归档

当 SZCA 的 CA 密钥对到期后，密钥对将被归档保存至少 5 年。归档的 CA 密钥对保存在本 CPS 6.2.1 所述的硬件密模块中，当其保存期满时，SZCA 将按照本 CPS 6.2.10 所述方法进行安全的销毁，确保私钥在销毁后不能被复原或重组。

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 密钥进行备份。当 CA 密钥对需导入保存到其他硬件密码模块，而在不同的硬件密码模块间进行传输时，必须进行对密钥对进行加密，并且在传递前要进行模块间的相互身份鉴别。另外 SZCA 设立有严格的密钥管理流程对 CA 密钥备份、传输进行控制，防止 CA 私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

通过硬件产生的订户签名私钥不能导出密码模块；其他方法产生的订户加密私钥可以在导出时采取加密的方式进行。

6.2.7 私钥存储于密码模块

私钥在硬件密码模块中加密保存。

6.2.8 激活私钥的方法

具有激活私钥权限的管理员、操作员使用加载有自己身份信息的加密 IC 卡登录，启动密钥管理程序，并进行激活私钥的操作，需要 3 名管理员同时在场监督。具体依照本 CPS 6.2.2 进行共同激活操作。

订户若使用软件产生、保存私钥,则私钥是保存在服务程序的软件密码模块中，这时订户使用口令保护私钥。当服务程序启动，软件加密模块被加载，密码模块验证口令完成后，私钥被激活。

当订户使用硬件密码模块产生、保存私钥时，订户使用硬件密码模块口令（或 pin 码）保护私钥，硬件加密模块被加载，密码模块验证口令完成后，私钥被激活。

6.2.9 解除私钥激活状态的方法

SZCA 私钥激活状态的解除，可以依照本 CPS 6.2.2 的方式进行，具有解除私钥激活状态权限的管理员使用加载有自己身份信息的加密 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。在硬件密码模块断电时，SZCA 私钥也将解除激活状态。

订户私钥在订户退出服务程序、系统或硬件软件模块断电的情况下，将取消激活。

6.2.10 销毁私钥的方法

具有销毁私钥权限的管理员使用加载有自己身份信息的加密 IC 卡登录，启动密钥管理程序，对所有的密钥的备份或其他硬件模块中的密钥副本进行销毁私钥的操作，需要 3 名管理员同时在场监督。且归档的私钥在归档期限结束后，再依照前述程序进行安全销毁操作。

6.2.11 密码模块的评估

由国家密码管理部门负责。

6.3 密钥对管理的其他方面

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 证书与密钥对使用的有效期

SZCA 根证书有效期一般为 5 年，CA 密钥使用有效期与根证书有效期一致。订户证书的有效期不超过 SZCA 密钥对的使用周期。 订户证书有效期通常为 1-3 年，订户密钥有效期一般与其证书有效期相同。密钥对到期后，不能再用作签名或加密；仅在签名验证时，证书的操作周期结束密钥对的公钥仍可继续使用，或对在证书有效期内加密的信息进行解密，私钥的使用期限可以在证书的有效期限以外。

6.4 激活数据

6.4.1 激活数据的产生与安装

CA 私钥的激活数据，必须按照本 CPS 6.2.2 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；并保证生成、安装激活数据的程序是安全可靠的，防止私钥被泄露、窃取、篡改或其他非经授权的使用和披露等。

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

6.4.2 激活数据的保护

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

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

6.4.3 激活数据的其它方面

（1）口令或 PIN 码应确保订户本人或其授权人员知悉，传递要采用一定的安全保密措施，防止泄露或窃取；

（2）在怀疑口令或 PIN 码可能泄露时，应更改激活数据，并销毁之前的记录；

（3）用于保护私钥或者密钥存储介质的口令、PIN 码，建议订户根据业务应用的需要定期更换；

（4）订户激活数据的销毁应由订户本人进行，且需确保他人无法通过残余信息、存储介质直接或间接恢复激活数据。

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；SZCA 系统部署在多级不同访问权限的防火墙之内，确保系统网络安全。

电子认证服务机构应制定全面、完善的安全管理策略和制度，通过严格的安全控制手段，确保电子认证服务机构软件和存储数据文件的系统是安全、可信赖的系统，不会受到未经授权的内部和外部访问。

电子认证服务机构应建立严格的管理体系来控制和监视运行系统，以防止未授权的修改。

电子认证服务机构应采用多级防火墙、入侵检测、安全审计、病毒防范系统等措施来保护电子认证服务机构网络环境的安全，适时更新版本，定期针对网络环境进行风险评估和审计，以检测有否被入侵的危险，尽可能降低来自网络的风险。

电子认证服务机构处理废旧设备时，必须清除影响认证业务安全性的信息存储并加以确认。

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。

SZCA 的主要安全技术和控制措施包括：采用安全可信任的操作系统、严格的身份识别和人员访问控制制度、多层防火墙设置、人员职责分割、内部操作控制、业务持续计划等各方面。

6.5.2 计算机安全评估

SZCA 的认证服务系统，通过国家密码管理局的安全性审查；使用的密码设备是通过国家密码管理局批准制造生产的。

电子认证服务机构应按照《粤港两地电子签名证书互认办法》要求，定期聘请独立第三方机构进行包括计算机和网络安全在内的整体评估；并根据整改意见进行系统的升级改造。

6.6 生命周期技术控制

6.6.1 系统开发控制

SZCA 的系统由国家相关的安全标准和具有密码产品及设备开发生产资质的可靠开

发商开发，其开发过程符合国家密码管理局及 SZCA 系统管理的各项规定。

6.6.2 安全管理控制

SZCA 认证服务系统的信息安全管理，严格遵循行业主管部门工业和信息化部、国家密码管理局的规范进行操作。系统的任何改造升级等变更，都须经过严格的测试验证后才能进行安装和使用。SZCA 认证业务系统的配置以及任何升级和维护都会记录在案，并实行严格控制，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。

SZCA 制定规范的系统开发、升级和维护工作程序，采取有效的控制措施，并适时作出修改或更新。这些程序及措施的内容应包括但不限于：

（1）无论由 SZCA 工作人员或特殊情况下的其它机构进行开发工作，均能使用一致和有效的内部标准；

（2）将生产及开发的环境分隔开的有效程序；

（3）将操作、运维、开发人员的职责得以区分的有效程序；

（4）对用于生产及开发的环境内的资料及系统进行有效访问的控制措施；

（5）对变更控制程序（包括但不限于系统和数据的正常和紧急变更）的有效控制措施（包括但不限于版本的控制、严格的测试验证等）；

（6）系统上线前进行安全性的检查和评估的程序，检查和评估内容包括有否安全漏洞和被入侵的危险等；

（7） 对采购设备及服务进行妥善管理的有效程序。

6.6.3 生命期的安全控制

SZCA 的系统及使用的密码产品、设备，都是由符合国家相关安全标准和具有商用密码产品生产资质的可靠开发商开发，其开发过程符合国家密码主管部门的相关要求。上述开发商的产品和服务，支持软硬件设备的持续升级，能满足证书及私钥生命期内可靠性安全性持续保障的要求。

6.7 网络安全控制

SZCA 设置多级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。此外，还安装入侵检测、防病毒等产品且定期升级，多方面对网络系统进行保护。

6.8 时间戳

SZCA 对各种系统日志、操作日志都将进行准确的时间标识，包括日期和时间。

7. 证书、证书吊销列表和在线证书状态协议

7.1 证书

SZCA 使用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。

SZCA 保证证书所采用的技术和证书结构符合《粤港两地电子签名证书互认办法》和《粤港两地电子签名证书互认技术标准列表和采用措施》的规定。SZCA 采用具体技术方案时应考虑证书跨境使用所需的互联互通需求。

SZCA 根据《ITU X.509》（第三版）（ITUX.509 v3）的证书格式发出及管理公钥证书，并根据《ITU X.509》（第二版）（ITU X.509 v2）的证书吊销列表格式生成及公布证书吊销列表。

SZCA 须在与某类型、种类的证书对应的 CPS 中明确说明所采用的证书结构（包括证书扩展项）及所包含的技术标准（例如包括采用何种数字符代码）。

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 证书项标准

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。

7.1.3 证书扩展项

7.1.3.1 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。

7.1.3.2 自定义扩展项

针对不同的证书应用服务，SZCA 适当增加并赋予其特定意义的扩展项。

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。

7.1.4 算法对象标识符

SZCA 签发粤港互认证书，密码算法的标识符为 RSA sha128、RSAsha256 和 SM2 三种。

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，其识别名称不允许匿名或者伪名，必须是有确定含义的识别名称。

7.1.7 证书策略及对象标识符

表 7.1-证书对象标识符

证书类别	工信部的对象标识符
个人证书	2.16.156.339.1.1.1.2.1
机构证书	2.16.156.339.1.1.2.2.1

7.2 证书吊销列表

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

7.2.1 版本

SZCA 的证书吊销列表采用 X.509 v2 版的证书格式。

7.2.2 CRL 项与 CRL 条目扩展项

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 sha2RSA 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(即它含有已吊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 http://www.szca.com 下载 CRL。

7.3 在线证书状态协议

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

SZCA 证书用户可以通过 SZCA 网站 http://www.szca.com 下载 CRL。或通过 SZCA 提供的服务地址由系统自动下载 CRL。

7.3.1 OCSP 请求

一个 OCSP 状态请求包括以下域：

Version：客户端使用 OCSP 协议的版本号； SZCA 在线证书状态协议为 v1 版。

Request or Name：为可选项，表示发起请求的实体名（DN）。

Request List：表示一个请求序列。

Signature Algorithm：为可选项，标识对本请求信息签名的算法。

Signature：为可选项，本请求信息的数字签名。

Certs：为可选项，请求状态的证书序列。

7.3.2 OCSP 响应

当一个确定的 OCSP 的响应消息包含以下域：

Version：OCSP 响应者使用的 OCSP 协议版本号；SZCA 的在线证书状态协议为 v1 版。

Responder ID：响应者实体的公钥的消息摘要或者响应者的 DN。

Produced At：该响应生成的日期和时间；

Responses：包含对每一个请求的响应序列，每个单独响应包含以下域。

Response Extensions：为可选项，指明响应中含有的 OCSP 扩展项。

Signature Algorithm：响应者对该响应消息签名所采用的算法；

Signature：本响应消息的数字签名。

Certs：为可选项，包含被请求状态的实际证书的一个序列。

7.3.3 OCSP 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 request Extensions 变量和响应消息中的 Response Extension 变量中包含一次性随机数，防止重放攻击。

CRL 引用：该扩展项指明一个 CRL，在该 CRL 中可以找到已经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。

8.认证机构审计与其它评估

8.1 评估的频率或情形

SZCA 可以针对运营及服务开展以下两种评估：

（1）外部评估

SZCA 按照《粤港两地电子签名证书互认办法》的要求，以《粤港两地电子签名证书互认的证书策略》为依据，每年聘请独立第三方机构进行 CPS 执行情况的审查。

对执行审查报告中提出的例外情况、不足之处或建议，SZCA 将及时作出回应，并适时提交包括改善和预防措施的整改计划书。

此外，SZCA 还将根据《中华人民共和国电子签名法》、《电子认证服务管理办法》及《电子认证密码服务管理办法》的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。

（2）内部评估

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

8.2 评估者的资质

SZCA 签发并管理粤港互认证书，需接受粤港电子签名证书互认试点工作组（以下简称粤港互认工作组）的评估，并定期聘请工信部等认可的第三方专业服务机构或主体，对 SZCA 执行本 CPS 的情况进行审查并出具报告。

SZCA 聘请的第三方专业服务机构须具备如下条件：

（1）处于工信部或国家有关部门认可的专业服务机构或人员名单之列，或持有国家认可的专业资质证书；

（2）在业界享有良好的声誉，具独立审计的职业素质，与本公司无影响审计的利害关系；

（3）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；

（4）具备检查系统运行性能的专业技术和工具。

SZCA 的内部评审，由 SZCA 运营安全管理小组负责组织协调，由经验丰富的熟悉电子认证业务和 PKI 技术的高级管理人员及核心技术人员等构成。

8.3 评估者与被评估者的关系

第三方评估者与 SZCA 之间没有任何的业务、财务往来，或者其它任何利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对 SZCA 进行评估。

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

8.4 评估内容

对 SZCA 评估内容包括但不限于：

（1）人事审查；

（2） 物理环境建设及安全运营管理规范审查；

（3） 系统结构及其运营审查；

（4）密钥管理审查；

（5）身份鉴别审核及证书处理流程审查；

（6）认证申请材料等记录、日志保存是否符合规定；

（7）CPS 的执行情况等。

8.5 对问题与不足采取的措施

针对行业主管部门工信部、粤港互认工作组及其认可的第三方审计机构的评估，

SZCA 将根据评估结果检查缺失和不足，提交纠正改进和预防措施以及整改计划书，并接受其对整改计划的审查，以及对整改情况的再次评估。

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

SZCA 将根据普遍认可的国际惯例或行业法律规范要求迅速解决问题。

8.6 评估结果的传达与发布

对于主管部门及第三方机构的审查评估结果，SZCA 将按法律及 CPS 要求将评估结果传达至本机构各相关职能部门及下属的注册机构，督促各部门按照处理结果及整改安排进行服务改进。

对于工信部、及其授权的粤港互认工作组等监管部门的评估、处理结果，SZCA 接受上述部门发布评估结果的决定；而对于第三方机构或人员的审计情况及结果，除非法律规定或情况特殊，如发生涉及公共利益有关 SZCA 服务运营资质的重大问题，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

9.1.1 证书签发与更新费用

根据市场、物价部门及行业主管部门的规定，SZCA 将收取合理的证书及相关服务费用，并在订户向 SZCA 订购证书时，提前告知订户 SZCA 证书签发及更新的收费项目、标准与方式。

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

9.1.2 证书查询费用

SZCA 暂不收取此项收费，但保留对此项服务收费的权利。

9.1.3 证书状态信息查询费用

SZCA 暂不收取此项收费，但保留对此项服务收费的权利。

9.1.4 其它服务费用

SZCA 保留收取其他服务费的权利。

9.1.5 退款策略

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

订户应当提供符合 SZCA 要求的完整、真实、准确的证书申请信息，否则 SZCA 对此造成的损失和后果不承担任何责任。

9.2 财务责任

9.2.1 保险范围

SZCA 根据业务发展情况决定其投保策略，目前暂无。

9.2.2 其他资产

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

9.2.3 对最终实体的保险与担保

目前，SZCA 仅根据《中华人民共和国电子签名法》的规定，对于由于 SZCA 的原因给订户造成的直接损失予以限额赔偿。根据订户所使用的证书的类型，赔付的额度有所不同，具体的赔付标准同本 CPS 9.8。

在适当的情况下，SZCA 不排除安排采购适当的保险或作出符合监管部门要求其他方式的赔偿安排（例如赔偿保证存款金）。并将在信息库中发布该订户有关保险的保险号或其他存在证据。当主管部门或独立第三方机构在审查中提出要求时，SZCA 将配合提交该保险号或上述保险的存在证据。

9.3 业务信息保密

9.3.1 保密信息范围

保密信息包括但不限于以下内容：

（1）SZCA 与 SZCA 授权的注册机构之间、SZCA 及其授权的注册机构与订户之间、SZCA 与其它证书服务相关方、SZCA 关联方之间的协议、往来函和商务协定等；

（2）与证书持有者证书公钥配对的私钥；

（3）SZCA 的审计日志及其他审计文件等；

（4）有关 SZCA 认证体系的运营信息；

（5）灾备计划、应急方案、安全措施等内部流程管制文件；

（6）订户证书信息以外的非公开信息等。

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

9.3.2 非保密信息

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

（2）证书持有者证书中包括的相关公开信息；

（3）证书状态及吊销列表信息；

（4）其他可以通过公共、公开渠道获得的信息。

虽然上述属非保密信息，并不意味着其能够被第三方任意不被授权的商业性使用，对于利用非保密信息的第三方主体，SZCA 和信息的所有人保留追究其法律责任的权利。

其它：SZCA 信息的保密性取决于特殊的数据项和申请。

9.3.3 保护保密信息的责任

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

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

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

当 SZCA 按照法律法规、司法机关裁判文书的要求，必须披露具有保密性质的信息

时，SZCA 可以向执法部门披露相关的保密信息。这种披露不视为违反保密的要求和义务。

9.4 个人信息保密

9.4.1 隐私保护方案

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

任何人选择使用 SZCA 的任何服务，就意味着表示已经同意接受 SZCA 有关隐私保护的制度。

9.4.2 作为隐私处理的信息

SZCA 在管理和使用订户申请、注册证书时提供的相关信息时，除了证书已经包括的信息及证书状态信息外，该订户的基本信息和身份认证资料，非经订户同意，或法律法规作出规定，及相关司法机关裁判要求，绝对不会任意对外公开。

9.4.3 非隐私的个人信息

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

9.4.4 保护隐私的责任

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

当 SZCA 在任何法律法规或者司法机关在合法程序的要求下，或者信息所有者书面授权的情况下，SZCA 可以向特定对象披露相关的隐私信息。这种披露不被视为违反隐私保护义务。包括与披露行为相关的或由此引发的损失，SZCA 无须为此承担任何责任。

9.4.5 使用隐私信息的告知与同意

SZCA 在其认证业务范围内使用所获得的任何订户信息，只用于订户身份识别、管理证书和服务订户的目的。在使用这些信息时，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司法机关、行政执法机关等有权机关通过合法程序的要求下，或者信息所有者书面授权的情况下向特定对象披露隐私信息时，也没有告知订户的义务，并且不需得到订户的同意。

SZCA 与其授权注册机构如果需要将订户隐私信息用于双方约定的用途以外的目的，在法律允许的情况下，事前需告知订户并征得其书面同意，获得经订户签章的书面授权文书。

9.4.6 依法进行信息披露

除非符合下列条件之一，否则 SZCA 绝对不会将订户的基本注册资料和身份认证信息提供给任何第三方主体：

（1）侦查机关，如公安机关、国家安全机关及检察院因案件侦查需要，向 SZCA 提出要求的；

（2）获得司法机关授权的诉讼案件当事人，向 SZCA 提出要求的；

（3）法院为执行有关证书纠纷的裁决或仲裁机构作出的申请法院执行的裁决，法院提出申请；

（4）国家行政执法机关为合法行政管理的需要，向 SZCA 要求的。

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

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

9.4.7 其他信息披露情形

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

其它信息披露亦需在法律法规和订户协议许可范围内。

9.5 知识产权

SZCA 享有并保留对证书以及 SZCA 提供的全部软件、文档、数据的独占的知识产权，包括保证证书和软件的完整权、冠名权、著作权和利益分享权等。

所有与 SZCA 发行的证书和 SZCA 提供的软件相关的一切版权、商标和其它知识产权均属于 SZCA 所有，上述知识产权包括但不限于相关的 SZCA 的规范性文件、CP/CPS、技术支持文件和使用手册等各种数据、信息、资料。SZCA 的其他电子认证服务机构在征得 SZCA 的授权同意后，可以使用相关的文件和手册。

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

9.6 陈述与担保

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

9.6.1 电子认证服务机构的陈述与担保

9.6.1.1 SZCA 对于自身服务的一般性陈述

(1) 建立电子认证业务规则（CPS）和其它认证服务所必需的规范、制度体系；

(2) 建立符合国家有关规定、行业标准的信息基础设施提供认证服务；

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

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

(5) SZCA 及其授权证书注册机构，是可观中立的第三方证书服务机构。

SZCA 不是证书订户或依赖方任意一方的代理人、受托人、管理人或其它代表。SZCA 和证书订户的关系，以及依赖方的关系并不是代理人和委托者的关系。证书订户和依赖方无权以合同形式或其它方法要求 SZCA 承担信托责任。SZCA 也不能用明示、暗示或其它方式，做出与上述规定相反的陈述。

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

9.6.1.2 SZCA 对订户的陈述与担保

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

（1）证书中没有 SZCA 所知的或源于 SZCA 的错误陈述；

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

（3）签发给订户的证书符合本 CPS 及其 CP 的实质性要求；

（4）将按本证书策略及相关电子认证业务规则的规定，及时吊销或挂起证书，并将证书的状态信息及时发布到 CRL 及 OCSP 上；

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

9.6.1.3 SZCA 对依赖方的陈述与担保

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

（1）除未经验证的订户信息外，证书中或证书指向的相关信息都是准确的；

具体来说，有关证书内容及状态信息，SZCA 可向依赖方提供以下保证：

第一，证书拥有者的合法存在性；

第二，证书拥有者的身份经过有效识别；

第三，证书中关于证书拥有者信息的准确性；

第三，证书状态 7*24 小时可查询；

第四，CA 根据 CPS 规则，废止不符合生效条件的证书。

（2）完全遵照本 CPS 及其 CP 的规定签发证书；

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

（4）及时吊销及挂起证书，并更新证书的状态信息。

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

9.6.2 注册机构的陈述与担保

经 SZCA 合法程序获得授权的注册机构 RA 保证：

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

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

② 注册机构应在合理的时间内完成证书申请处理。在申请者提交资料齐全且符合要求的情况下，处理证书申请的时间为 5 个工作日；

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

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

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

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

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

（4）依据本 CPS 的规定，确保运营系统处在安全的物理环境中，并具备相应的安全管理和隔离措施。RA 必须能够对证书服务相关的全部数据资料进行备份；

（5）按照 SZCA 的要求，保证其与下级证书服务机构间的信息传输安全。并且 RA 承诺严格执行为所有证书用户提供隐私保密的义务，并愿意承担因此而带来的法律责任。

（5） 接受 SZCA 根据本 CPS 和授权协议对 RA 进行管理，包括接受服务资质审核和规范执行检查，根据相关协议内容配合 SZCA 需要的电子认证业务合规性审计。 承认 SZCA 对所有证书服务申请者的服务请求拥有最终处理权。

（6）为证书申请者提供必要的服务及技术咨询。

9.6.3 订户的陈述与担保

订户一旦接受 SZCA 及其授权注册机构签发的证书，自接受之时起直至证书的使用有效期满为止，如果订户不另行通知，则订户需向 SZCA 及所有合理信赖证书中所含信息的依赖方，做出如下承诺和保证：

（1）申请证书时所提交的所有证书申请材料、信息，包括申请过程中订户所陈述、声明的信息，是完整、真实和准确的，可供 SZCA 及相关依赖方检查和核实；并且愿意

承担任何提供虚假、伪造等信息的法律责任；

如果存在代理人，订户和代理人两者负有无限连带责任。 作为订户，有责任就因申请代理人的疏忽所作的任何不实陈述、错误陈述或遗漏，及时通知通知 SZCA 或其下属发证机构，申请吊销证书或重新申请证书或申请证书更新（包含密钥更新）。

（2）订户保证在证书有效期内所有包含在证书中的有关信息是真实、完整的；一旦证书所含的订户有关信息发生改变，应及时通知 SZCA;

订户通过下载或者从 SZCA 证书服务机构处获取证书后，应先测试使用检查证书中所含信息是否正确，如果有失误或者遗漏，应在合理的期间内通过 SZCA 提供的联系方式通知 SZCA。一旦接受并使用证书，即表明订户承诺就订户所知道的或注意到的包含在证书中的信息，都是真实的。如果订户发现证书中信息失实或者有错误或者遗漏，应停止使用证书，并及时通知 SZCA 并申请证书更新（或证书密钥更新）；

申请资料、信息发生变更时应及时通知 SZCA，申请证书变更。且在订户未通知给发证机构之前的期间，SZCA 及其发证机构有理由认为：订户认为上述信息都是真实的。

（3）用与证书中所含公钥相对应的私钥所进行的每一次签名，都是订户本人进行的或经其授权所进行的操作，并且在进行签名时，证书是有效证书（证书没有过期、挂起或吊销）并已被订户接受；并在能力范围内保证在未经授权的人员从未访问过订户私钥。

（4）证书将按本 CPS 的规定，只用于经过授权的或其它符合法律及 CPS 规定的使用目的。

订户保证，其证书使用是符合国家法律法规规定，按照该类型证书所对应的 CPS 的规定，并且是按照相关的用户/订户协议约定的证书使用条件和范围操作该证书的，并且对该证书的使用是按照订户本人的真实意愿，或者按照订户的委托授权用于为其处理事务。

除非经订户和发证机构的书面协议明确约定，否则，订户保证不得将证书用于 SZCA 及其发证机构（或类似机构）所从事的证书签发业务等，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。

（5）保证密钥生成、保存及使用的安全性，及私钥失密、冒用盗用时的通知义务

一经接受证书，意味着订户既知悉和接受本 CPS 中的所有条款，又知悉和接受相应的订户协议，并愿意承担上述文件中的法律责任。则订户就应承当如下责任：采用可靠的方式生成密钥对，采取安全措施保证私钥的安全存储，始终保持对其私钥的使用控制，保证私钥及其存储介质与设备的保密性，使用可靠的系统，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。

订户应保证本人对于证书私钥的控制，不得任意交于他人占有、使用或随意告知他人使用私钥的方法，否则需自行承担私钥被盗用冒用的法律责任；并且一旦发现因自身疏忽造成密钥泄露、遗失等，或发生非自身原因造成的私钥被非法破坏、篡改、使用的失密情况，应立即停止证书的使用，及时通知 SZCA 及依赖方，申请对证书进行挂起或吊销操作。

（6）证书被吊销或挂起时停止使用证书

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

总之，一经接受证书，订户即同意使 SZCA 免于承担因下列原因直接或间接造成的任何责任和损失：

① 订户（或其授权的代理人）虚假地或错误地陈述了事实；

② 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隐瞒，构成对 SZCA 和其他依赖方的欺骗；

③ 订户没有使用可信系统或没有采用必要的合理的安全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。

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

9.6.4 依赖方的陈述与担保

依赖方在信赖任何 SZCA 签发的证书时，就意味着保证：

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

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

（3）在信赖 SZCA 签发的证书前，已经对证书进行过合理的检查和审核，包括：检查 SZCA 公布的最新的 CRL 获得该证书的状态，确认该证书没有被挂起或吊销；检查该证书信任路径中所有出现过的证书的可靠性；检查该证书的有效期以及适用范围；检查其它能够影响证书有效性的信息；

一旦由于疏忽或者其它原因未履行合理检查的义务，依赖方愿意承担因此造成的自身或他人的损失，并且就此对 SZCA 带来的损失进行补偿。

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

（5）信任证书前确认证书记载内容与信任所需的证明是一致的；

（6）依赖方须承担因未履行以上责任所产生的法律责任。

9.6.5 其它参与方的陈述与担保

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

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

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

能够达到准确验证鉴别身份的效果。

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

9.7 担保免责

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

（1）由于如 9.16.4 所列的不可抗力因素导致 SZCA 暂停、终止部分或全部数字证书服务，SZCA 不承担赔偿责任；

（2）订户违反本 CPS 9.6.3 之承诺时，SZCA 得以免除承担责任；

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

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

② 订户或依赖方没有使用可靠安全的系统来使用证书；

③ 订户或依赖方没有履行妥善保管私钥的义务；

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

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

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

（5）在订户提出证书挂起或吊销请求后，到 SZCA 实际完成吊销或挂起该证书的

期间，如果该证书被用以进行非法交易，或者发生其他相关证书使用纠纷的，如果 SZCA 按照本 CPS 的规范进行有关操作，SZCA 不承担任何损害赔偿责任；

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

9.8 SZCA 的赔偿责任及其限制

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

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

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

1. 个人类证书，不超过 800 元；

2. 机构类证书，不超过 4000 元；

3. 设备类证书，不超过 8000 元。

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

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

9.9 订户和依赖方的赔偿责任

9.9.1 订户的赔偿责任

有下列情形之一的，订户应承担相应的损失赔偿责任：

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

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

（3）订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有通知依赖方、SZCA 及其授权的证书服务机构；

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

（5）将私钥及证书不当交付他人使用，造成 SZCA、依赖方遭受损害的；

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

（7）证书被吊销（包含但不限于证书到期）、挂起期间仍然使用证书；

（8）其他订户使用证书违反本 CPS 及相关操作规范的情形。

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

SZCA 与订户签署的协议另有赔偿规定的，从其规定。

9.9.2 依赖方的赔偿责任

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

体的损失进行赔偿。

9.10 有效期与终止

9.10.1 有效期限

本 CPS 自发布之日起正式生效，文档中将详细注明版本号及发布日期，最新版本的 CPS 请访问 SZCA 网站下载获取，对具体个人不做另行通知，新发布的 CPS 自动取代废止旧 CPS。

9.10.2 终止

本 CPS 及其更新版本在 SZCA 终止电子认证服务时失效。在终止服务六十日前向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，如电话、电子邮件、信函、传真等，个别通知订户、依赖方。订户或依赖方如有需要，也可以通过 SZCA 的联系方式向 SZCA 咨询了解 SZCA 终止的相关业务处理情况。

9.12 修订

9.12.1 修订程序

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

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

9.12.2 通知机制与期限

SZCA 有权修订本 CPS 中任何术语和条款，而且无须预先通知任何一方。

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

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

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

9.12.3 修订同意

对于业务内容、各方责任义务等进行调整的重大修订，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，将被视为同意该修订，该 15 日期满修订后的 CPS 即行生效。

而对于联系方式及其他文字性的修改等非重大修订，自发布之日起生效。

9.12.4 必须修改业务规则的情形

如果出现下列情况，必须对 CPS 进行修订：

（1）密码技术出现重大发展，导致现有的 CPS 内容滞后性、不适应性；

（2）有关认证业务的相关标准发生改变；

（3）认证系统和有关管理规范发生重大升级或改变；

（4）法律法规和主管部门的要求；

（5）现有 CPS 出现重要缺陷；

（6）应用出现新的要求等。

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

9.13 争议处理

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

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

9.14 管辖法律

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

有关证书、证书策略及具体类型证书对应的 CPS 的任何争议，包括适用、解释、有效性等各种争议，无论订户或依赖方居住于何地或者其在何处使用证书，都应适用证书签发地，也即 SZCA 及其注册机构所在地（住所地），尤其是主要办事机构所在地或经常居所地的法律。则有关 SZCA 的证书、CP 及 CPS 的各种争议，都应统一适用中国的法律，无论当事人是否在合同中约定法律适用条款。

9.15 与适用法律的符合性

SZCA 的各项策略均遵守并符合中华人民共和国各项法律法规和国家信息主管部门的要求。若本 CPS 中的任意条款被主管部门宣布为非法、不可执行或无效时，SZCA 将对该不符合性条款进行修订，直至该条款合法有效可执行为止。但本 CPS 某一条款或某些条款等部分条款的无效，不影响其它条款的法律效力。

9.16 一般条款

9.16.1 完整协议

本 CPS 将替代先前的与该主题相关的书面或口头说明、解释，并与订户协议、依赖方协议及其他补充协议构成 SZCA 与各方参与者之间的完整协议。

9.16.2 转让

若 SZCA 因不可抗力或其他原因暂停、终止电子认证服务，SZCA 的订户需按法律规定接受相应接管 CA 的证书服务的安排。

除以上原因外，SZCA、订户及依赖方之间的责任和义务不得以任何形式转让。

9.16.3 分割性

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

9.16.4 强制执行

无

9.16.5 不可抗力

本 CPS 提及的不可抗力是指“不能预见、不能避免和不能克服的客观情况”。

不可抗力主要包括但不限于以下几种情形：

（1）自然灾害、如台风、洪水、冰雹；

（2）政府行为，如征收、征用；

（3）社会异常事件，如战争、政变、罢工、骚乱；

（4）互联网或其他基础设施无法使用等。

9.17 其它条款

SZCA 对本 CPS 拥有最终解释权。